2/5/1 (Item 1 from file: 351)
DIALOG(R)File 351:DERWENT WPI

012070618 **Image available**
WPI Acc No: 98-487529/**199842**
XRPX Acc No: N98-381072
Authentication method for encrypted communication system - involves generating first and second authentication information based on random number, confidential information, predefined algorithm which are compared to authenticate validity of first station
Patent Assignee: OKI ELECTRIC IND CO LTD (OKID)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
JP 10210023 A		19980807	JP 9712876	A	19970127	H04L-009/08	199842 B

Priority Applications (No Type Date): JP 9712876 A 19970127
Patent Details:

Patent	Kind	Lan	Pg	Filing Notes	Application	Patent
JP 10210023 A			42			

Abstract (Basic): JP 10210023 A
The method involves storing common confidential information (Ka,K'a) in memories (13,43), respectively for each station. A first station transmits an information `Ia'. Either the first or a second station generates a random number `r' and transmits to other station. The first station generates a first authentication information based on the random number, confidential information and a predetermined algorithm.
Similarly, the second station generates a second authentication information based on random number, confidential information and predetermined algorithm. The second station then compares both the first and second authentication information and authenticates the information generated at the first station.
ADVANTAGE - Prevents tapping in case of separate communication. Eliminates using communicated information again.
Dwg.1/20
Title Terms: AUTHENTICITY; METHOD; ENCRYPTION; COMMUNICATE; SYSTEM; GENERATE; FIRST; SECOND; AUTHENTICITY; INFORMATION; BASED; RANDOM; NUMBER ; CONFIDE; INFORMATION; PREDEFINED; ALGORITHM; COMPARE; AUTHENTICITY; VALID; FIRST; STATION
Derwent Class: W01
International Patent Class (Main): H04L-009/08
International Patent Class (Additional): H04L-009/32
File Segment: EPI

2/5/2 (Item 1 from file: 347)
DIALOG(R)File 347:JAPIO

05926923 **Image available**
AUTHENTICATION METHOD, CIPHER KEY SHARING METHOD, AND COMMUNICATION SYSTEM

PUB. NO.: 10-210023 A]
PUBLISHED: August 07, 1998 (19980807)
INVENTOR(s): SAI TAKAO
NAKAGAWA SATOSHI
NAKAI TOSHIHISA
TORII TAKASHI
APPLICANT(s): OKI ELECTRIC IND CO LTD [000029] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 09-012876 [JP 9712876]

FILED: January 27, 1997 (19970127)
INTL CLASS: [6] H04L-009/08; H04L-009/32
JAPIO CLASS: 44.3 (COMMUNICATION -- Telegraphy); 44.2 (COMMUNICATION -- Transmission Systems)

ABSTRACT

PROBLEM TO BE SOLVED: To provide a new method which makes a second station authenticate a first station in a communication system including first and second stations which desire communication.

SOLUTION: Secret information K(sub a) (K'(sub a)) common to a first station 11 and a second station 41 is stored in storage parts 13 and 43 of respective stations. The first station 11 transmits user information I(sub a) identifying the first station to the second station 41. One of first and second stations generates random numbers (r) and transmits them to the other. The first station 11 uses random numbers, secret information, and a prescribed algorithm to generate first authentication information and transmits it to the second station 41. The second station 41 uses random numbers, secret information and a prescribed algorithm to generate second authentication information. The second station 41 compares first and second authentication information with each other and discriminates whether they coincide with each other or not to authenticate the validity of the first station.

1

【特許請求の範囲】

【請求項１】　共通の秘密情報をそれぞれの記憶手段に格納している第１の局および第２の局を含む通信システムにおいて、前記第２の局が前記第１の局を認証するに当たり、

前記第１の局が、第１の局である旨を示すユーザ情報を前記第２の局に送信する処理と、

前記第１および第２の局のいずれか一方が、乱数を発生しこれを他方の局に送信する処理と、

前記第１の局が、前記乱数と自局内の前記記憶手段に格納している前記秘密情報とを入力とする所定のアルゴリズムにより第１の認証情報を生成しこれを前記第２の局に送信する処理と、

前記第２の局が、前記乱数と自局内の前記記憶手段に格納している前記秘密情報とを入力とする所定のアルゴリズムにより第２の認証情報を生成する処理と、

前記第２の局が、前記第１の認証情報と前記第２の認証情報とを比較することにより前記第１の局の正当性を認証する処理とを含むことを特徴とする認証方法。

【請求項２】　共通の秘密情報をそれぞれの記憶手段に格納している第１の局および第２の局を含む通信システムにおいて、前記第２の局が前記第１の局を認証するに当たり、

前記第１の局が、第１の局である旨を示すユーザ情報を第２の局に送信する処理と、

前記第１の局が、乱数を発生する処理と、

前記第１の局が、該乱数を前記第２の局に送信する処理と、

前記第１の局が、前記乱数と自局内の前記記憶手段に格納してある前記秘密情報とを入力とする所定のアルゴリズムにより第１の認証情報を生成しこれを前記第２の局に送信する処理と、

前記第２の局が、前記送信されてきた乱数を認証する処理と、

前記乱数を認証する処理にて前記乱数が正当でないとされた場合に実行され、前記第２の局が前記第１の局を正当でないとする処理と、

前記乱数を認証する処理にて前記乱数が正当であるとされた場合に実行され、前記第２の局が、前記乱数と自局内の前記記憶手段に格納してある前記秘密情報とを入力とする所定のアルゴリズムにより第２の認証情報を生成し、かつ、前記第１の認証情報と前記第２の認証情報とを比較することにより前記第１の局の正当性を認証する処理とを含むことを特徴とする認証方法。

【請求項３】　共通の秘密情報をそれぞれの記憶手段に格納している第１の局および第２の局を含む通信システムにおいて、前記第２の局が前記第１の局を認証するに当たり、

前記第１の局が、第１の局である旨を示すユーザ情報を前記第２の局に送信する処理と、

2

前記第１および第２の局のいずれか一方が乱数を発生しこれを他方の局に送信する処理と、

前記第１の局が、前記第２の局をアクセスした回数を計数すると共に該アクセス回数を前記第２の局に送信する処理と、

前記第１の局が、前記乱数と前記アクセス回数と自局内の前記記憶手段に格納してある前記秘密情報とを入力とする所定のアルゴリズムにより第１の認証情報を生成しこれを前記第２の局に送信する処理と、

前記第２の局が、前記送信されてきたアクセス回数を認証する処理と、

前記アクセス回数を認証する処理にて前記アクセス回数が正当でないとされた場合に実行され、前記第２の局が前記第１の局を正当でないとする処理と、

前記アクセス回数を認証する処理にて前記アクセス回数が正当であるとされた場合に実行され、前記第２の局が、前記乱数と前記アクセス回数と自局内の前記記憶手段に格納してある前記秘密情報とを入力とする所定のアルゴリズムにより第２の認証情報を生成し、かつ、前記第１の認証情報と前記第２の認証情報とを比較することにより前記第１の局の正当性を認証する処理とを含むことを特徴とする認証方法。

【請求項４】　共通の秘密情報をそれぞれの記憶手段に格納している第１の局および第２の局を含む通信システムにおいて、前記第２の局が前記第１の局を認証するに当たり、

前記第１の局が、第１の局である旨を示すユーザ情報を前記第２の局に送信する処理と、

前記第１の局が、乱数を発生する処理と、

前記第１の局が、自局内の前記記憶手段に格納してある前記秘密情報を鍵として前記乱数と前記ユーザ情報とを暗号化することにより認証情報を生成しこれを前記第２の局に送信する処理と、

前記第２の局が、自局内の前記記憶手段に格納してある前記秘密情報を鍵として前記送信されてきた認証情報を復号化する処理と、

前記第２の局が、前記復号化で得たユーザ情報と前記送信されてきたユーザ情報とを比較すること、および、前記復号化で得た乱数を認証することにより前記第１の局の正当性を認証する処理とを含むことを特徴とする認証方法。

【請求項５】　共通の秘密情報をそれぞれの記憶手段に格納している第１の局および第２の局を含む通信システムにおいて、前記第２の局が前記第１の局を認証するに当たり、

前記第１の局が、第１の局である旨を示すユーザ情報を前記第２の局に送信する処理と、

前記第１の局が第１の乱数および第２の乱数を発生する処理と、

前記第１の局が、第１の乱数を前記第２の局に送信する

処理と、
前記第１の局が、前記第２の乱数を鍵として前記ユーザ情報を暗号化して第１の暗号文を生成する処理と、
前記第１の局が、前記第１の乱数と自局内の前記記憶手段に格納してある前記秘密情報とを入力とする所定のアルゴリズムにより認証情報を生成するための暗号アルゴリズムの鍵を生成する処理と、
前記第１の局が、前記暗号アルゴリズムの鍵を用いて前記第２の乱数と前記第１の暗号文とをさらに暗号化して第２の暗号文を生成しこれを認証情報として前記第２の局に送信する処理と、
前記第２の局が、前記送信されてきた第１の乱数を認証する処理と、
前記第１の乱数を認証する処理にて前記第１の乱数が正当でないとされた場合に実行され、前記第２の局が前記第１の局を正当でないとする処理と、
前記第１の乱数を認証する処理にて前記第１の乱数が正当であるとされた場合に実行され、前記第２の局が、前記第１の乱数と自局内の前記記憶手段に格納してある前記秘密情報とを入力とする所定のアルゴリズムにより認証情報を復号化するための鍵を生成し、該鍵を用い前記送信されてきた認証情報を復号化し、該復号化で得たユーザ情報と前記送信されてきたユーザ情報とを比較することにより前記第１の局の正当性を認証する処理とを含むことを特徴とする認証方法。

【請求項６】　共通の秘密情報をそれぞれの記憶手段に格納している第１の局および第２の局を含む通信システムにおいて、前記第２の局が前記第１の局を認証するに当たり、
前記第１の局が、第１の局である旨を示すユーザ情報を前記第２の局に送信する処理と、
前記第１の局が、乱数を発生する処理と、
前記第１の局が、前記第２の局をアクセスした回数を計数する処理と、
前記第１の局が、前記乱数を鍵として前記ユーザ情報と前記アクセス回数とを暗号化する処理と、
前記第１の局が、自局内の前記記憶手段に格納してある前記秘密情報を鍵として前記暗号化されたユーザ情報と前記アクセス回数とをさらに暗号化してこれを認証情報として前記第２の局に送信する処理と、
前記第２の局が、自局内の前記記憶手段に記憶してある前記秘密情報を鍵として前記送信されてきた認証情報を復号化する処理と、
前記第２の局が、前記復号化で得たユーザ情報と前記送信されてきたユーザ情報とを比較すること、および、前記復号化で得たアクセス回数を認証することにより前記第１の局の正当性を認証する処理とを含むことを特徴とする認証方法。

【請求項７】　共通の秘密情報をそれぞれの記憶手段に格納している第１の局および第２の局を含む通信システムにおいて、前記第２の局が前記第１の局を認証するに当たり、
前記第１の局が、第１の局である旨を示すユーザ情報を前記第２の局に送信する処理と、
前記第１の局が、第１の乱数および第２の乱数を発生する処理と、
前記第１の局が、該第１の乱数を前記第２の局に送信する処理と、
前記第１の局が、前記第２の局をアクセスした回数を計数する処理と、
前記第１の局が、前記第２の乱数を鍵として前記ユーザ情報と前記アクセス回数とを暗号化して第１の暗号文を生成する処理と、
前記第１の局が、前記第１の乱数と自局内の前記記憶手段に格納してある前記秘密情報とを入力とする所定のアルゴリズムにより認証情報を生成するための暗号アルゴリズムの鍵を生成する処理と、
前記第１の局が、前記暗号アルゴリズムの鍵を用いて前記第２の乱数と前記第１の暗号文とをさらに暗号化して第２の暗号文を生成しこれを認証情報として前記第２の局に送信する処理と、
前記第２の局が、前記第１の乱数と自局内の前記記憶手段に格納してある前記秘密情報とを入力とする所定のアルゴリズムにより前記認証情報を復号化するための鍵を生成する処理と、
前記第２の局が、前記復号化するための鍵を用い前記送信されてきた認証情報を復号化する処理と、
前記復号化で得たユーザ情報と前記送信されてきたユーザ情報とを比較すること、および、前記復号化で得たアクセス回数を認証することにより前記第１の局の正当性を認証する処理とを含むことを特徴とする認証方法。

【請求項８】　通信を希望する第１の局および第２の局と、該第２の局に代わって認証をする信頼できる第３の局とを含み、前記第１の局および第３の局は共通の秘密情報をそれぞれの記憶手段に格納している通信システムにおいて、前記第３の局が前記第１の局を認証するに当たり、
前記第１の局が、第１の局である旨を示すユーザ情報を前記第２の局に送信する処理と、
前記第１の局が、乱数を発生する処理と、
前記第１の局が、乱数を前記第２の局に送信する処理と、
前記第１の局が、前記乱数と自局内の前記記憶手段に格納してある前記秘密情報とを用いて認証情報を生成しこれを前記第２の局に送信する処理と、
前記第２の局が、前記第１の局から送信されてきたユーザ情報と乱数と認証情報とを前記第３の局に送信する処理と、
前記第３の局が、前記乱数と前記第２の局から送信されてきた認証情報を自局内の前記記憶手段に格納してある

5

前記秘密情報を用いて認証することにより前記第１の局の正当性を認証する処理と、
前記第３の局が、認証結果を前記第２の局に送信する処理とを含むことを特徴とする認証方法。
【請求項９】　通信を希望する第１の局および第２の局と、該第２の局に代わって認証をする信頼できる第３の局とを含み、前記第１の局および第３の局は共通の秘密情報をそれぞれの記憶手段に格納している通信システムにおいて、前記第３の局が前記第１の局を認証するに当たり、
前記第１の局が、第１の局である旨を示すユーザ情報を前記第２の局に送信する処理と、
前記第２の局が、前記ユーザ情報を受信すると乱数を発生し該乱数を前記第１の局に送信する処理と、
前記第１の局が、前記第２の局から送信されてきた乱数と自局内の前記記憶手段に格納している前記秘密情報とを用いて認証情報を生成しこれを前記第２の局に送信する処理と、
前記第２の局が、前記乱数と前記第１の局から送信されてきたユーザ情報と認証情報とを前記第３の局に送信する処理と、
前記第３の局が、前記第２の局から送信されてきた認証情報を自局内の前記記憶手段に格納してある前記秘密情報を用いて認証することにより前記第１の局の正当性を認証する処理と前記第３の局が、認証結果を前記第２の局に送信する処理とを含むことを特徴とする認証方法。
【請求項１０】　通信を希望する第１の局および第２の局と、これら局間に介在する中間局とを含み、前記第１の局および第２の局は共通の秘密情報をそれぞれの記憶手段に格納している通信システムにおいて、前記第２の局が前記第１の局を認証するに当たり、
前記第１の局が、第１の局である旨を示すユーザ情報を前記中間局に送信する処理と、
前記中間局が、前記ユーザ情報を受信すると乱数を発生し該乱数を前記第１の局に送信する処理と、
前記第１の局が、前記中間局から送信されてきた乱数と自局内の前記記憶手段に格納している前記秘密情報とを用いて認証情報を生成しこれを前記中間局に送信する処理と、
前記中間局が、前記乱数と前記第１の局から送信されてきたユーザ情報と認証情報とを前記第２の局に送信する処理と、
前記第２の局が、前記中間局から送信されてきた認証情報を自局内の前記記憶手段に格納している前記秘密情報を用いて認証することにより前記第１の局の正当性を認証する処理とを含むことを特徴とする認証方法。
【請求項１１】　請求項１～３のいずれか１項に記載の認証方法において、
前記第１の局および第２の局それぞれに、前記所定のアルゴリズムとして用いることができるアルゴリズムを複

6

数種かつ同様に予め用意しておき、
前記第１または第２の局が選択信号を発生しこれに応じ前記第１および第２の局それぞれが前記複数種のアルゴリズムの中から１つを選択し、
該選択されたアルゴリズムにより前記第１の局は前記第１の認証情報を生成し、前記第２の局は前記第２の認証情報を生成することを特徴とする認証方法。
【請求項１２】　請求項２に記載の認証方法において、前記送信されてきた乱数を認証する処理とは、
前記第１の局から送信されてくる乱数の履歴を記憶し、かつ、今回の通信で前記第１の局から送信されてきた乱数が前回の通信までの乱数履歴中に含まれているか否かを調べる処理であることを特徴とする認証方法。
【請求項１３】　請求項４に記載の認証方法において、前記復号化で得た乱数を認証する処理とは、
復号化で得られる乱数の履歴を記憶し、かつ、今回の通信での復号化で得られた乱数が前回の通信までの乱数履歴中に含まれているか否かを調べる処理であることを特徴とする認証方法。
【請求項１４】　請求項５に記載の認証方法において、前記送信されてきた第１の乱数を認証する処理とは、
前記第１の局から送信されてくる第１の乱数の履歴を記憶し、かつ、今回の通信で前記第１の局から送信された第１の乱数が前回の通信までの乱数履歴中に含まれているか否かを調べる処理であることを特徴とする認証方法。
【請求項１５】　請求項３に記載の認証方法において、前記送信されてきたアクセス回数を認証する処理とは、
前記第１の局から送信される前記アクセス回数を記憶し、かつ、今回の通信で前記第１の局から送信されたアクセス回数が前回の通信までのアクセス回数に対し所定の不等式関係を満たすか否かを調べる処理であることを特徴とする認証方法。
【請求項１６】　請求項６または７に記載の認証方法において、
前記復号化で得たアクセス回数を認証する処理とは、
前記第２の局が復号化で得たアクセス回数を記憶し、かつ、今回の通信での復号化で得たアクセス回数が前回の通信での復号化で得たアクセス回数に対し所定の不等式関係を満たすか否かを調べる処理であることを特徴とする認証方法。
【請求項１７】　請求項５または７に記載の認証方法において、
前記第１の局および第２の局それぞれに、前記所定のアルゴリズムとして用いることができるアルゴリズムを複数種かつ同様に予め用意しておき、
前記第１または第２の局が選択信号を発生しこれに応じ前記第１および第２の局それぞれが前記複数種のアルゴリズムの中から１つを選択し、
該選択されたアルゴリズムにより、前記第１の局は前記

暗号アルゴリズムの鍵を生成し、前記第２の局は前記認証情報を復号化するための鍵を生成することを特徴とする認証方法。

【請求項１８】　請求項１、２、３、５、７、１１または１７に記載の認証方法において、

前記所定のアルゴリズムを一方向性関数とすることを特徴とする認証方法。

【請求項１９】　請求項４～７のいずれか１項に記載の認証方法において、

前記第１の局および第２の局それぞれに、前記認証情報を生成する際のアルゴリズムおよび前記認証情報を復号化する際のアルゴリズムとして用いることができる複数種の暗号アルゴリズムを同様に予め用意しておき、

前記第１または第２の局が選択信号を発生しこれに応じ前記第１および第２の局それぞれが前記複数種の暗号アルゴリズムの中から１つを選択し、

該選択された暗号アルゴリズムにより、前記第１の局は前記認証情報を生成する暗号化をし、前記第２の局は前記認証情報を復号化することを特徴とする認証方法。

【請求項２０】　請求項１～３のいずれか１項に記載の認証方法により前記第１の局について認証をし、

該認証により正当とされた場合は前記第１の局および第２の局それぞれで前記乱数および前記秘密情報を入力とする所定の暗号鍵生成アルゴリズムにより共有暗号鍵をそれぞれ生成し、

これを前記第１および第２の局の共有暗号鍵とすることを特徴とする暗号鍵共有方法。

【請求項２１】　請求項４または６に記載の認証方法により前記第１の局について認証をし、

該認証により正当とされた場合は前記第１の局および第２の局それぞれで前記乱数を入力とする所定の暗号鍵生成アルゴリズムにより共有暗号鍵をそれぞれ生成し、

これを前記第１および第２の局の共有暗号鍵とすることを特徴とする暗号鍵共有方法。

【請求項２２】　請求項５または７に記載の認証方法により前記第１の局について認証をし、

該認証により正当とされた場合は前記第１の局および第２の局それぞれで前記第２の乱数を入力とする所定の暗号鍵生成アルゴリズムにより共有暗号鍵をそれぞれ生成し、

これを前記第１および第２の局の共有暗号鍵とすることを特徴とする暗号鍵共有方法。

【請求項２３】　請求項２０～２２のいずれか１項に記載の暗号鍵共有方法において、

前記第１の局および第２の局それぞれに、前記所定の暗号鍵生成アルゴリズムとして用いることができるアルゴリズムを複数種かつ同様に予め用意しておき、

前記第１または第２の局が選択信号を発生しこれに応じ前記第１および第２の局それぞれが前記複数種の暗号鍵生成アルゴリズムの中から１つを選択し、

該選択された暗号鍵生成アルゴリズムにより、前記第１の局および第２の局は共有暗号鍵をそれぞれ生成することを特徴とする暗号鍵共有方法。

【請求項２４】　請求項８または９に記載の認証方法により前記第１の局について認証をし、

該認証により正当とされた場合は前記第１の局および第３の局それぞれで共有暗号鍵をそれぞれ生成し、

前記第３の局は該共有暗号鍵を前記第２の局に送信しこれを前記第２の局は共有暗号鍵とすることを特徴とする暗号鍵共有方法。

【請求項２５】　請求項１０に記載の認証方法により前記第１の局について認証をし、

該認証において正当とされた場合は、前記第１の局および第２の局それぞれで共有暗号鍵をそれぞれ生成し、

これを前記第１および第２の局の共有暗号鍵とすることを特徴とする暗号鍵共有方法。

【請求項２６】　共通の秘密情報をそれぞれの記憶手段に格納している第１の局および第２の局を含む通信システムにおいて、

(1) 前記第１の局から前記第２の局に第１の局である旨を示すユーザ情報を送信するためのユーザ情報送信手段と、

(2) 前記第１の局または前記第２の局に設けられ、乱数を発生するための乱数生成手段と、

(3) 前記発生された乱数を他方の局に送信するための乱数送信手段と、

(4) 前記第１の局に設けられ、前記乱数と自局内の前記記憶手段に格納された前記秘密情報とを入力とする所定のアルゴリズムにより第１の認証情報を生成するための第１の認証情報生成手段と、

(5) 前記第１の認証情報を前記第２の局に送信するための認証情報送信手段と、

(6) 前記第２の局に設けられ、前記乱数と自局内の前記記憶手段に格納された前記秘密情報とを入力とする所定のアルゴリズムにより第２の認証情報を生成するための第２の認証情報生成手段と、

(7) 前記第２の局に設けられ、前記第１の認証情報と前記第２の認証情報とを比較することで前記第１の局の正当性を認証するための認証手段とを具えたことを特徴とする通信システム。

【請求項２７】　共通の秘密情報をそれぞれの記憶手段に格納している第１の局および第２の局を含む通信システムにおいて、

(1) 前記第１の局から前記第２の局に第１の局である旨を示すユーザ情報を送信するためのユーザ情報送信手段と、

(2) 前記第１の局に設けられ、乱数を発生するための乱数生成手段と、

(3) 前記発生された乱数を前記第２の局に送信するための乱数送信手段と、

(4) 前記第１の局に設けられ、前記乱数と自局内の前記記憶手段に格納された前記秘密情報とを入力とする所定のアルゴリズムにより第１の認証情報を生成するための第１の認証情報生成手段と、
(5) 前記第１の認証情報を前記第２の局に送信するための認証情報送信手段と、
(6) 前記第２の局に設けられ、前記送信されてくる乱数を認証するための乱数認証手段と、
(7) 前記第２の局に設けられ、前記送信されてくる乱数と自局内の前記記憶手段に格納された前記秘密情報とを入力とする所定のアルゴリズムにより第２の認証情報を生成するための第２の認証情報生成手段と、
(8) 前記第２の局に設けられ、前記第１の認証情報と前記第２の認証情報とを比較することにより前記第１の局の正当性を認証するための認証手段とを具えたことを特徴とする通信システム。

【請求項２８】　共通の秘密情報をそれぞれの記憶手段に格納している第１の局および第２の局を含む通信システムにおいて、
(1) 前記第１の局から前記第２の局に第１の局である旨を示すユーザ情報を送信するためのユーザ情報送信手段と、
(2) 前記第１の局または前記第２の局に設けられ、乱数を発生するための乱数生成手段と、
(3) 前記発生された乱数を他方の局に送信するための乱数送信手段と、
(4) 前記第１の局に設けられ、前記第１の局が前記第２の局をアクセスしたアクセス回数を計数するためのアクセス回数計数手段と、
(5) 前記アクセス回数を前記第２の局に送信するためのアクセス回数送信手段と、
(6) 前記第１の局に設けられ、前記アクセス回数と前記乱数と自局内の前記記憶手段に格納された前記秘密情報とを入力とする所定のアルゴリズムにより第１の認証情報を生成するための第１の認証情報生成手段と、
(7) 前記第１の認証情報を前記第２の局に送信するための認証情報送信手段と、
(8) 前記第２の局に設けられ、前記送信されてくるアクセス回数を認証するためのアクセス回数認証手段と、
(9) 前記第２の局に設けられ、前記送信されてくるアクセス回数と前記乱数と自局内の前記記憶手段に格納された前記秘密情報とを入力とする所定のアルゴリズムにより第２の認証情報を生成するための第２の認証情報生成手段と、
(10) 前記第２の局に設けられ、前記第１の認証情報と前記第２の認証情報とを比較することで前記第１の局の正当性を認証するための認証手段とを具えたことを特徴とする通信システム。

【請求項２９】　共通の秘密情報をそれぞれの記憶手段に格納している第１の局および第２の局を含む通信システムにおいて、
(1) 前記第１の局から前記第２の局に第１の局である旨を示すユーザ情報を送信するためのユーザ情報送信手段と、
(2) 前記第１の局に設けられ、乱数を発生するための乱数生成手段と、
(3) 前記第１の局に設けられ、自局内の前記記憶手段に格納してある前記秘密情報を鍵として前記乱数と前記ユーザ情報とを暗号化することにより認証情報を生成するための認証情報生成手段と、
(4) 前記認証情報を前記第２の局に送信するための認証情報送信手段と、
(5) 前記第２の局に設けられ、自局内の前記記憶手段に格納してある前記秘密情報を鍵として前記送信されてくる認証情報を復号化するための認証情報復号化手段と、
(6) 前記第２の局に設けられ、前記復号化により得られたユーザ情報と前記送信されてくるユーザ情報とを比較すること、および、前記復号化により得られた乱数を認証することにより前記第１の局の正当性を認証するための認証手段とを具えたことを特徴とする通信システム。

【請求項３０】　共通の秘密情報をそれぞれの記憶手段に格納している第１の局および第２の局を含む通信システムにおいて、
(1) 前記第１の局から前記第２の局に対し第１の局である旨を示すユーザ情報を送信するためのユーザ情報送信手段と、
(2) 前記第１の局に設けられ、第１の乱数および第２の乱数を発生するための乱数生成手段と、
(3) 前記発生された第１の乱数を前記第２の局に送信するための乱数送信手段と、
(4) 前記第１の局に設けられ、前記第２の乱数を鍵として前記ユーザ情報を暗号化して第１の暗号文を生成するための暗号文生成手段と、
(5) 前記第１の局に設けられ、前記第１の乱数と自局内の前記記憶手段に格納してある前記秘密情報とを入力とする所定のアルゴリズムにより認証情報を生成するための暗号アルゴリズムの鍵を生成するための暗号鍵生成手段と、
(6) 前記第１の局に設けられ、前記暗号アルゴリズムの鍵を用いて前記第２の乱数と前記第１の暗号文とをさらに暗号化して認証情報としての第２の暗号文を生成するための認証情報生成手段と、
(7) 前記認証情報を前記第２の局に送信するための認証情報送信手段と、
(8) 前記第２の局に設けられ、前記送信されてくる第１の乱数を認証するための乱数認証手段と、
(9) 前記第２の局に設けられ、前記送信されてくる第１の乱数と自局内の前記記憶手段に格納してある前記秘密情報とを入力とする所定のアルゴリズムにより前記認証情報を復号化するための鍵を生成するための復号鍵生成

手段と、

(10)前記第２の局に設けられ、前記復号鍵を用いて前記認証情報を復号化するための認証情報復号化手段と、

(11)前記第２の局に設けられ、前記復号化により得られたユーザ情報と前記送信されてくるユーザ情報とを比較することにより前記第１の局の正当性を認証するための認証手段とを具えたことを特徴とする通信システム。

【請求項３１】　共通の秘密情報をそれぞれの記憶手段に格納している第１の局および第２の局を含む通信システムにおいて、

(1) 前記第１の局から前記第２の局に対し第１の局である旨を示すユーザ情報を送信するためのユーザ情報送信手段と、

(2) 前記第１の局に設けられ、乱数を発生するための乱数生成手段と、

(3) 前記第１の局に設けられ、前記第１の局が前記第２の局をアクセスしたアクセス回数を計数するためのアクセス回数計数手段と、

(4) 前記第１の局に設けられ、前記乱数を鍵として前記ユーザ情報と前記アクセス回数とを暗号化するための暗号化手段と、

(5) 前記第１の局に設けられ、自局内の前記記憶手段に格納してある前記秘密情報を鍵として前記暗号化されたユーザ情報とアクセス回数とをさらに暗号化することにより認証情報を生成するための認証情報生成手段と、

(6) 前記認証情報を前記第２の局に送信するための認証情報送信手段と、

(7) 前記第２の局に設けられ、自局内の前記記憶手段に格納してある前記秘密情報を鍵として前記送信されてくる認証情報を復号化するための認証情報復号化手段と、

(8) 前記第２の局に設けられ、前記復号化により得られるユーザ情報と前記送信されてくるユーザ情報とを比較すること、および、前記復号化により得られるアクセス回数を認証することにより前記第１の局の正当性を認証するための認証手段とを具えたことを特徴とする通信システム。

【請求項３２】　共通の秘密情報をそれぞれの記憶手段に格納している第１の局および第２の局を含む通信システムにおいて、

(1) 前記第１の局から前記第２の局に対し第１の局である旨を示すユーザ情報を送信するためのユーザ情報送信手段と、

(2) 前記第１の局に設けられ、第１の乱数および第２の乱数を発生するための乱数生成手段と、

(3) 前記発生された第１の乱数を前記第２の局に送信するための乱数送信手段と、

(4) 前記第１の局に設けられ、前記第１の局が前記第２の局をアクセスしたアクセス回数を計数するためのアクセス回数計数手段と、

(5) 前記第１の局に設けられ、前記第２の乱数を鍵として前記ユーザ情報と前記アクセス回数とを暗号化して第１の暗号文を生成するための暗号文生成手段と、

(6) 前記第１の局に設けられ、前記第１の乱数と自局内の前記記憶手段に格納してある前記秘密情報とを入力とする所定のアルゴリズムにより認証情報を生成するための暗号アルゴリズムの鍵を生成するための暗号鍵生成手段と、

(7) 前記第１の局に設けられ、前記暗号アルゴリズムの鍵を用いて前記第２の乱数と前記第１の暗号文とをさらに暗号化して認証情報としての第２の暗号文を生成するための認証情報生成手段と、

(8) 前記認証情報を前記第２の局に送信するための認証情報送信手段と、

(9) 前記第２の局に設けられ、前記送信されてくる第１の乱数と自局内の前記記憶手段に格納してある前記秘密情報とを入力とする所定のアルゴリズムにより前記認証情報を復号化するための鍵を生成するための復号鍵生成手段と、

(10)前記第２の局に設けられ、前記送信されてくる認証情報を前記復号鍵を用い復号化するための認証情報復号化手段と、

(11)前記第２の局に設けられ、前記復号化により得られるユーザ情報と前記送信されてくるユーザ情報とを比較すること、および、前記復号化により得られるアクセス回数を認証することにより前記第１の局の正当性を認証するための認証手段とを具えたことを特徴とする通信システム。

【請求項３３】　通信を希望する第１の局および第２の局と、該第２の局に代わって認証をする信頼できる第３の局とを含み、前記第１の局および第３の局は共通の秘密情報をそれぞれの記憶手段に格納している通信システムにおいて、

(1) 前記第１の局から前記第２の局に第１の局である旨を示すユーザ情報を送信するためのユーザ情報送信手段と、

(2) 前記第１の局に設けられ、乱数を発生するための乱数生成手段と、

(3) 前記発生された乱数を前記第２の局に送信するための乱数送信手段と、

(4) 前記第１の局に設けられ、前記乱数と自局内の前記記憶手段に格納された前記秘密情報とを用い認証情報を生成するための認証情報生成手段と、

(5) 前記認証情報を前記第２の局に送信するための認証情報送信手段と、

(6) 前記第１の局から前記第２の局に送信されてくる前記ユーザ情報、前記乱数および前記認証情報それぞれを前記第３の局に送信するための送信手段と、

(7) 前記第３の局に設けられ、前記第２の局から送信されてくる前記認証情報を自局内の前記記憶手段に格納してある前記秘密情報を用いて認証することにより前記第

13

１の局の正当性を認証するための認証手段と、
(8) 前記第３の局に設けられ、前記認証結果を前記第２の局に送信するための認証結果送信手段とを具えたことを特徴とする通信システム。
【請求項３４】　通信を希望する第１の局および第２の局と、該第２の局に代わって認証をする信頼できる第３の局とを含み、前記第１の局および第３の局は共通の秘密情報をそれぞれの記憶手段に格納している通信システムにおいて、
(1) 前記第１の局から前記第２の局に第１の局である旨を示すユーザ情報を送信するためのユーザ情報送信手段と、
(2) 前記第２の局に設けられ、前記ユーザ情報を受信すると乱数を発生するための乱数生成手段と、
(3) 前記発生された乱数を前記第１の局に送信するための乱数送信手段と、
(4) 前記第１の局に設けられ、前記乱数と自局内の前記記憶手段に格納された前記秘密情報とを用い認証情報を生成するための認証情報生成手段と、
(5) 前記認証情報を前記第２の局に送信するための認証情報送信手段と、
(6) 前記乱数と前記第１の局から前記第２の局に送信されてくる前記ユーザ情報および前記認証情報を前記第３の局に送信するための送信手段と、
(7) 前記第３の局に設けられ、前記第２の局から送信されてくる前記認証情報を自局内の前記記憶手段に格納してある前記秘密情報を用いて認証することにより前記第１の局の正当性を認証するための認証手段と、
(8) 前記第３の局に設けられ、前記認証結果を前記第２の局に送信するための認証結果送信手段とを具えたことを特徴とする通信システム。
【請求項３５】　通信を希望する第１の局および第２の局と、これら局間に介在する中間局とを含み、前記第１の局および第２の局は共通の秘密情報をそれぞれの記憶手段に格納している通信システムにおいて、
(1) 前記第１の局から前記中間局に第１の局である旨を示すユーザ情報を送信するためのユーザ情報送信手段と、
(2) 前記中間局に設けられ、前記ユーザ情報を受信すると乱数を発生するための乱数生成手段と、
(3) 前記発生された乱数を前記第１の局に送信するための乱数送信手段と、
(4) 前記第１の局に設けられ、前記送信されてくる乱数と自局内の前記記憶手段に格納してある前記秘密情報とを用いて認証情報を生成するための認証情報生成手段と、
(5) 前記認証情報を前記中間局に送信するための認証情報送信手段と、
(6) 前記乱数と第１の局から前記中間局に送信されてくる前記ユーザ情報および前記認証情報を前記第２の局に

14

送信するための送信手段と、
(7) 前記第２の局に設けられ、前記送信されてくる認証情報を自局内の前記記憶手段に格納してある前記秘密情報を用い認証することにより前記第１の局の正当性を認証するための認証手段とを具えたことを特徴とする通信システム。
【請求項３６】　請求項２６～２８のいずれか１項に記載の通信システムにおいて、
前記第１の局および第２の局それぞれに設けられかつ前記所定のアルゴリズムとして使用できるアルゴリズムを複数格納している記憶手段と、
前記第１の局および第２の局のいずれか一方でアルゴリズム選択信号を発生しこれを他方の局にも送信し、しかも、これら選択信号により前記第１の局および第２の局それぞれの前記複数のアルゴリズムを記憶している記憶手段から共通の１つのアルゴリズムをそれぞれ選択してこれをそれぞれの局に備わる前記第１または第２の認証情報生成手段に前記所定のアルゴリズムとして出力するアルゴリズム選択手段とを具えたことを特徴とする通信システム。
【請求項３７】　請求項２７に記載の通信システムにおいて、
前記乱数認証手段として、
前記第２の局に設けられ前記第１の局から送信されてくる乱数の履歴を記憶するための手段と、
前記第２の局に設けられ今回の通信で前記第１の局から送信されてくる乱数が前回の通信までの乱数履歴に含まれているか否かを調べるための比較手段とを含むことを特徴とする通信システム。
【請求項３８】　請求項２９に記載の通信システムにおいて、
前記復号化により得られた乱数を認証する手段として、
前記第２の局に設けられ、復号化で得られる乱数の履歴を記憶するための手段と、
前記第２の局に設けられ今回の通信での復号化で得られた乱数が前回の通信までの乱数履歴に含まれているか否かを調べるための比較手段とを含むことを特徴とする通信システム。
【請求項３９】　請求項３０に記載の通信システムにおいて、
前記第１の乱数を認証するための手段として、
前記第２の局に設けられ前記第１の局から送信されてくる第１の乱数の履歴を記憶するための手段と、
前記第２の局に設けられ今回の通信で前記第１の局から送信されてくる第１の乱数が前回の通信までの乱数履歴に含まれているか否かを調べるための比較手段とを含むことを特徴とする通信システム。
【請求項４０】　請求項２８に記載の通信システムにおいて、
前記アクセス回数認証手段として、

前記第２の局に設けられ、前記第１の局から送信されてくるアクセス回数を記憶するための手段と、
前記第２の局に設けられ今回の通信で前記第１の局から送信されてくるアクセス回数が前回の通信までのアクセス回数に対し所定の不等式関係を満たすか否かを調べるための比較手段とを含むことを特徴とする通信システム。

【請求項４１】　請求項３１または３２に記載の通信システムにおいて、
前記復号化で得られたアクセス回数を認証するための手段として、
前記第２の局に設けられ、復号化で得られるアクセス回数を記憶する手段と、
前記第２の局に設けられ今回の通信での復号化で得られた乱数が前回の通信での復号化で得られたアクセス回数に対し所定の不等式関係を満たすか否かを調べるための比較手段とを含むことを特徴とする通信システム。

【請求項４２】　請求項３０または３２に記載の通信システムにおいて、
前記第１の局および第２の局それぞれに設けられかつ前記所定のアルゴリズムとして使用できるアルゴリズムを複数格納している記憶手段と、
前記第１の局および第２の局のいずれか一方でアルゴリズム選択信号を発生しこれを他方の局にも送信し、しかも、これら選択信号により前記第１の局および第２の局それぞれの前記複数のアルゴリズムを記憶している記憶手段から共通の１つのアルゴリズムをそれぞれ選択してこれをそれぞれの局に備わる前記暗号鍵生成手段または復号鍵生成手段に前記所定のアルゴリズムとして出力するアルゴリズム選択手段とを具えたことを特徴とする通信システム。

【請求項４３】　請求項２６、２７、２８、３０、３２、３６または４２に記載の通信システムにおいて、
前記所定のアルゴリズムを一方向性関数とすることを特徴とする通信システム。

【請求項４４】　請求項２７に記載の通信システムにおいて、
前記乱数認証手段は、前記乱数が正当でないと判断した場合、前記第１の局を正当でないと決定し、
前記第２の認証情報生成手段および前記認証手段それぞれを、前記乱数認証手段が前記乱数を正当と判断した場合に動作する手段とすることを特徴とする通信システム。

【請求項４５】　請求項２８に記載の通信システムにおいて、
前記アクセス回数認証手段は、前記アクセス回数が正当でないと判断した場合、前記第１の局を正当でないと決定し、
前記第２の認証情報生成手段および前記認証手段それぞれを、前記アクセス回数認証手段が前記アクセス回数を正当と判断した場合に動作する手段とすることを特徴とする通信システム。

【請求項４６】　請求項３０に記載の通信システムにおいて、
前記第１の乱数認証手段は、前記第１の乱数が正当でないと判断した場合、前記第１の局を正当でないと決定し、
前記復号鍵生成手段、前記認証情報復号化手段および前記認証手段それぞれを、前記第１の乱数認証手段が前記第１の乱数を正当と判断した場合に動作する手段とすることを特徴とする通信システム。

【請求項４７】　請求項２９～３２のいずれか１項に記載の通信システムにおいて、
前記第１の局および第２の局それぞれに設けられかつ前記認証情報生成手段および前記認証情報復号化手段で使用できる暗号アルゴリズムを複数格納している記憶手段と、
前記第１の局および第２の局のいずれか一方でアルゴリズム選択信号を発生しこれを他方の局にも送信し、しかも、これら選択信号により前記第１の局および第２の局それぞれの前記複数の暗号アルゴリズムを記憶している記憶手段から共通の１つのアルゴリズムをそれぞれ選択してこれをそれぞれの局に備わる前記認証情報生成手段または認証情報復号化手段に出力するアルゴリズム選択手段とを具えたことを特徴とする通信システム。

【請求項４８】　請求項２６～２８のいずれか１項に記載の通信システムにおいて、
前記第１の局および第２の局それぞれに設けられ、前記認証手段により前記第１の局が正当であるとされた場合に動作し、前記乱数および前記秘密情報を入力とする暗号鍵生成アルゴリズムにより共有暗号鍵を生成する共有暗号鍵生成手段をさらに具えたことを特徴とする通信システム。

【請求項４９】　請求項２９または３１に記載の通信システムにおいて、
前記第１の局および第２の局それぞれに設けられ、前記認証手段により前記第１の局が正当であるとされた場合に動作し、前記乱数を入力とする暗号鍵生成アルゴリズムにより共有暗号鍵を生成する共有暗号鍵生成手段をさらに具えたことを特徴とする通信システム。

【請求項５０】　請求項３０または３２に記載の通信システムにおいて、
前記第１の局および第２の局それぞれに設けられ、前記認証手段により前記第１の局が正当であるとされた場合に動作し、前記第２の乱数を入力とする暗号鍵生成アルゴリズムにより共有暗号鍵を生成する共有暗号鍵生成手段をさらに具えたことを特徴とする通信システム。

【請求項５１】　請求項４８～５０のいずれか１項に記載の通信システムにおいて、
前記第１の局および第２の局それぞれに設けられ、前記

暗号鍵生成アルゴリズムとして用いることができるアルゴリズムを複数格納している記憶手段と、
前記第１の局および第２の局のいずれか一方でアルゴリズム選択信号を発生しこれを他方の局にも送信し、しかも、これら選択信号により前記第１の局および第２の局それぞれの前記複数の暗号アルゴリズムを記憶している記憶手段から共通の１つのアルゴリズムをそれぞれ選択してこれをそれぞれの局に備わる共有暗号鍵生成手段に出力する、アルゴリズム選択手段とを具えたことを特徴とする通信システム。

【請求項５２】　請求項３３または３４に記載の通信システムにおいて、
前記第１の局および第３の局それぞれに設けられ、前記認証手段により前記第１の局が正当であるとされた場合に動作する共有暗号鍵生成手段と、
前記第３の局で生成された共有暗号鍵を前記第２の局に送信するための共有暗号鍵送信手段とを具えたことを特徴とする通信システム。

【請求項５３】　請求項３５に記載の通信システムにおいて、
前記第１の局および第２の局それぞれに設けられ、前記認証手段により前記第１の局が正当であるとされた場合に動作する共有暗号鍵生成手段を具えたことを特徴とする通信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、通信を行う一対の通信者の間で通信相手を認証する方法と、暗号通信を行なう際の共有暗号鍵（暗号化用の鍵と復号化用の鍵が同一な暗号鍵）の作成方法と、その実施に好適な通信システムとに関するものである。

【０００２】

【従来の技術】暗号通信を行うとき、共有暗号鍵を通信者間でどのように共有するかが重要な問題の一つになる。例えば文献Ｉ（IEEE Trans. on Inform. Theory（アイイーイーイー トランザクション オン インフォメーション セオリ）, IT-22, No. 6, pp. 644-654(1976)）および文献Ｉを引用した文献II（「暗号と情報セキュリティ」，辻井　重男、笠原　正雄　編著、昭晃堂、pp. 72-73、(1990)）には、事前に秘密情報を共有せずに共有暗号鍵を生成する方法が開示されている。具体的には、通信者Ａ、Ｂが暗号鍵を交換したいと仮定する。大きい素数ｎ（５１２ビット程度）と、ｎ個の要素を持つ有限体ＧＦ（ｎ）の原始元である整数ｇとを公開して、次のように通信者Ａ、Ｂの共有暗号鍵を生成している。

【０００３】（１）Ａは乱数ｘを生成し、そしてＸ＝$g^x \bmod n$をＢに送信する。なお、$g^x \bmod n$とはg^xをｎで割った余りを表す（以下の$g^y \bmod n$などにおいて同様。）。

【０００４】（２）Ｂは乱数ｙを生成し、そしてＹ＝$g^y \bmod n$をＡに送信する。

【０００５】（３）Ａは$K_A = Y^x \bmod n$のように暗号鍵を生成する。

【０００６】（４）Ｂは$K_B = X^y \bmod n$のように暗号鍵を生成する。

【０００７】簡単な演算により、$K_A = K_B = g^{xy} \bmod n$を得ることができる。この値を通信者Ａ、Ｂの共有暗号鍵とする。一方、第３者がこの暗号鍵を解読する場合、これが離散対数問題であるため現実的な時間で解を求めることが難しい。したがって、通信者Ａ、Ｂ間での暗号鍵の共有を確保することができる。

【０００８】

【発明が解決しようとする課題】しかしながら上述した従来の方法では、通信相手を認証する方法が示されていない。

【０００９】そのため、通信相手の認証がなされないまま暗号鍵を生成することになる。したがって、例えば通信中に通信情報が第３者（正当でない通信者）に盗聴されて改竄されても、改竄された情報により暗号鍵が計算されてしまうので、暗号鍵を共有することができなくなる場合もある。

【００１０】したがって通信相手を認証するための新規な方法が望まれる。

【００１１】また、通信相手を認証するための新規な方法が開発されても、その新規な認証方法で認証作業が終えた後に別途に通信者間で暗号鍵共有のための情報通信を行なうのでは、その通信作業中にやはり第３者による盗聴や攻撃がなされてしまう危険がある。

【００１２】したがって通信相手を認証することと併せて通信者間の暗号鍵の共有も行なうことができる暗号鍵共有方法の実現が望まれる。

【００１３】また、上記の認証方法や暗号鍵共有方法の実施に好適な通信システムの実現が望まれる。

【００１４】

【課題を解決するための手段】

（１）．そこでこの出願の認証方法の第１の発明によれば、共通の秘密情報をそれぞれの記憶手段に格納している第１の局および第２の局を含む通信システムにおいて、前記第２の局が前記第１の局を認証するに当たり、以下の各処理を含むことを特徴とする。

【００１５】(a) 前記第１の局が、第１の局である旨を示すユーザ情報を前記第２の局に送信する処理。(b) 前記第１の局または第２の局が、乱数を発生してこれを他方の局に送信する処理。(c) 前記第１の局が、前記乱数と自局内の前記記憶手段に格納している前記秘密情報とを入力とする所定のアルゴリズムにより第１の認証情報を生成しこれを前記第２の局に送信する処理。(d) 前記第２の局が、前記乱数と自局内の前記記憶手段に格納している前記秘密情報とを入力とする所定のアルゴリズムにより第２の認証情報を生成する処理。(e) 前記第２の

局が、前記第１の認証情報と前記第２の認証情報とを比較することにより前記第１の局の正当性を認証する処理。

【００１６】ここで秘密情報は、第１の局と第２の局とで共有することができる予め定めた任意の秘密の情報である（以下の各発明において同じ。）。またユーザ情報は、第１の局に固有の任意の情報であり、例えばユーザＩＤや名前（人名などに限らない任意のもの）やメイルアドレスなどである（以下の各発明において同じ。）。

【００１７】この認証方法の第１の発明によれば、第１の局が第２の局にユーザ情報を送信すると認証動作が開始される。また認証は、第１の局および第２の局に共通な秘密情報、乱数および所定のアルゴリズムを用い各局が生成する第１および第２の認証情報の一致・不一致を判定することで、なされる。

【００１８】この認証方法の第１の発明を実施するため、以下の(1) ～(7) の手段を具えた通信システム（通信システムの第１の発明）を構成するのが好適である。

【００１９】(1) 前記第１の局から前記第２の局に第１の局である旨を示すユーザ情報を送信するためのユーザ情報送信手段。(2) 前記第１の局または前記第２の局に設けられ、乱数を発生するための乱数生成手段。(3) 前記発生された乱数を他方の局に送信するための乱数送信手段。(4) 前記第１の局に設けられ、前記乱数と自局内の前記記憶手段に格納された前記秘密情報とを入力とする所定のアルゴリズムにより第１の認証情報を生成するための第１の認証情報生成手段。(5) 前記第１の認証情報を前記第２の局に送信するための認証情報送信手段。(6) 前記第２の局に設けられ、前記乱数と自局内の前記記憶手段に格納された前記秘密情報とを入力とする所定のアルゴリズムにより第２の認証情報を生成するための第２の認証情報生成手段。(7) 前記第２の局に設けられ、前記第１の認証情報と前記第２の認証情報とを比較することで前記第１の局の正当性を認証するための認証手段。

【００２０】（２）．また、この出願の認証方法の第２の発明によれば、共通の秘密情報をそれぞれの記憶手段に格納している第１の局および第２の局を含む通信システムにおいて、前記第２の局が前記第１の局を認証するに当たり、以下の各処理を含むことを特徴とする。

【００２１】(a) 前記第１の局が、第１の局である旨を示すユーザ情報を前記第２の局に送信する処理。(b) 前記第１の局が、乱数を発生する処理。(c) 第１の局が、前記乱数を第２の局に送信する処理。(d) 前記第１の局が、前記乱数と自局内の前記記憶手段に格納してある前記秘密情報とを入力とする所定のアルゴリズムにより第１の認証情報を生成しこれを前記第２の局に送信する処理。(e) 前記第２の局が、前記送信されてきた乱数を認証する処理。(f) 前記乱数を認証する処理にて前記乱数が正当でないとされた場合に実行され、前記第２の局が前記第１の局を正当でないとする処理。(g) 前記乱数を認証する処理にて前記乱数が正当であるとされた場合に実行され、前記第２の局が、前記乱数と自局内の前記記憶手段に格納してある前記秘密情報とを入力とする所定のアルゴリズムにより第２の認証情報を生成し、かつ、前記第１の認証情報と前記第２の認証情報とを比較することにより前記第１の局の正当性を認証する処理。

【００２２】この認証方法の第２の発明によれば、第１の局が第２の局にユーザ情報および乱数を送信すると認証動作が開始される。また認証は、第１の局から送信されてきた乱数に対し先ず行なうことができる。乱数の認証は、例えば、第１の局から今回送信されてきた乱数が第１の局から過去に送られた乱数履歴に含まれているか否かを調べることにより行なうことが出来る。

【００２３】乱数の認証は次の様な役目をもつ。第３者が通信情報を盗聴し、これを用いて第２の局を繰り返し攻撃したとしても、これは既に使用された乱数を用いた攻撃である。するとこの乱数は上記乱数履歴に存在するので、第２の局は、この攻撃を、第３者によるものと判断することができる。そのため第３者による不当な繰り返し攻撃を見つけることができるので、第３者による通信システムへのそれ以上の侵入を防止することができる。しかも、乱数認証において第１の局を正当でないと第２の局が判定した場合は、第２の局側での認証情報作成処理を省略できる。したがって、第２の局が第３者の攻撃により占有される程度を軽減することができる。

【００２４】また、乱数が正当と判断された場合は、第２の局は第２の認証情報の生成と、第１および第２の認証情報の比較とを行なうので、正当な通信相手の認証は第１の発明と同様に正確におこなうことができる。

【００２５】なお、この認証方法の第２の発明において情報を送信する各処理は、それぞれを別々に行なうことを必須とする意味ではない。通信回数を減らす意味から、情報処理に支障がない範囲で、いくつかの送信処理を同時に行ってももちろん良い。例えば、ユーザ情報、乱数および認証情報は同時に送信することができる。

【００２６】この認証方法の第２の発明を実施するため、以下の(1) ～(8) の手段を具えた通信システム（通信システムの第２の発明）を構成するのが好適である。

【００２７】(1) 前記第１の局から前記第２の局に第１の局である旨を示すユーザ情報を送信するためのユーザ情報送信手段。(2) 前記第１の局に設けられ、乱数を発生するための乱数生成手段。(3) 前記発生された乱数を前記第２の局に送信するための乱数送信手段。(4) 前記第１の局に設けられ、前記乱数と自局内の前記記憶手段に格納された前記秘密情報とを入力とする所定のアルゴリズムにより第１の認証情報を生成するための第１の認証情報生成手段。(5) 前記第１の認証情報を前記第２の局に送信するための認証情報送信手段。(6) 前記第２の局に設けられ、前記送信されてくる乱数を認証するため

の乱数認証手段。(7) 前記第２の局に設けられ、前記送信されてくる乱数と自局内の前記記憶手段に格納された前記秘密情報とを入力とする所定のアルゴリズムにより第２の認証情報を生成するための第２の認証情報生成手段。(8) 前記第２の局に設けられ、前記第１の認証情報と前記第２の認証情報とを比較することにより前記第１の局の正当性を認証するための認証手段。

【００２８】（３）．また、この出願の認証方法の第３の発明によれば、共通の秘密情報をそれぞれの記憶手段に格納している第１の局および第２の局を含む通信システムにおいて、前記第２の局が前記第１の局を認証するに当たり、以下の各処理を含むことを特徴とする。

【００２９】(a) 前記第１の局が、第１の局である旨を示すユーザ情報を第２の局に送信する処理。(b) 前記第１の局または第２の局が、乱数を発生してこれを他方の局に送信する処理。(c) 前記第１の局が、前記第２の局をアクセスした回数を計数すると共に該アクセス回数を前記第２の局に送信する処理。(d) 前記第１の局が、前記乱数と前記アクセス回数と自局内の前記記憶手段に格納してある前記秘密情報とを入力とする所定のアルゴリズムにより第１の認証情報を生成しこれを前記第２の局に送信する処理。(e) 前記第２の局が、前記送信されてきたアクセス回数を認証する処理。(f) 前記アクセス回数を認証する処理にて前記アクセス回数が正当でないとされた場合に実行され、前記第２の局が前記第１の局を正当でないとする処理。(g) 前記アクセス回数を認証する処理にて前記アクセス回数が正当であるとされた場合に実行され、前記第２の局が、前記乱数と前記アクセス回数と自局内の前記記憶手段に格納してある前記秘密情報とを入力とする所定のアルゴリズムにより第２の認証情報を生成し、かつ、前記第１の認証情報と前記第２の認証情報とを比較することにより前記第１の局の正当性を認証する処理。

【００３０】この認証方法の第３の発明によれば、第１の局が第２の局にユーザ情報、乱数およびアクセス回数を送信すると認証動作が開始される。また認証は、第１の局から送信されてきたアクセス回数に対し先ず行なうことができる。アクセス回数の認証は、例えば、前回の送信の際に第１の局から送信されてきたアクセス回数をn'_a、第１の局から今回送信されてきたアクセス回数をn_a、通信ミスなどを考慮した数をεとしたとき、$n'_a + \varepsilon > n_a > n'_a$という不等式関係を満たすか否かを調べることにより行なうことが出来る。

【００３１】アクセス回数の認証は次の様な役目をもつ。第３者が通信情報を盗聴し、これを用いて第２の局を繰り返し攻撃したとしても、この攻撃で送信されてくるアクセス回数は既に送られてきた値と同じである。すると上記不等式関係を満たさないので、第２の局は、この攻撃を、第３者によるものと判断することができる。そのため第３者による不当な繰り返し攻撃を見つけることができるので、第３者による通信システムへのそれ以上の侵入を防止することができる。しかも、アクセス回数の認証において第１の局を正当でないと第２の局が判定した場合は、第２の局側での認証情報作成処理を省略できる。このため、第３者の攻撃により第２の局が占有される程度を軽減することができる。

【００３２】また、上記の第２の発明では過去に使用した乱数を記憶する必要があるのに対し、この第３の発明ではアクセス回数を記憶するだけで済むので、第２の発明に比べメモリを節約することができる。

【００３３】また、アクセス回数が正当と判断された場合は、第２の局は第２の認証情報の生成と、第１および第２の認証情報の比較とを行なうので、正当な通信相手の認証を正確におこなうことができる。

【００３４】またこの第３の発明の場合では、認証情報は乱数、アクセス回数、秘密情報および所定のアルゴリズムにより生成するので、第１発明に比べさらに詳細な認証を行なうことができる。

【００３５】なお、この認証方法の第３の発明を実施するに当たり、好ましくは第１の局が乱数を発生し第２の局に送信するのが良い。こうすると、ユーザ情報を送信する際に乱数も一緒に送信することができる。一方、第２の局が乱数を発生する手順にした場合は、第１の局側が認証情報を生成するために必須の乱数を第２の局から第１の局に別途に送信する処理が必要になるので、第１の局が乱数を発生する場合に比べて通信回数が増えてしまう。

【００３６】この認証方法の第３の発明を実施するため、以下の(1) ～(10)の手段を具えた通信システム（通信システムの第３の発明）を構成するのが好適である。

【００３７】(1) 前記第１の局から前記第２の局に第１の局である旨を示すユーザ情報を送信するためのユーザ情報送信手段。(2) 前記第１の局または前記第２の局に設けられ、乱数を発生するための乱数生成手段。(3) 前記発生された乱数を他方の局に送信するための乱数送信手段。(4) 前記第１の局に設けられ、前記第１の局が前記第２の局をアクセスしたアクセス回数を計数するためのアクセス回数計数手段。(5) 前記アクセス回数を前記第２の局に送信するためのアクセス回数送信手段。(6) 前記第１の局に設けられ、前記アクセス回数と前記乱数と自局内の前記記憶手段に格納された前記秘密情報とを入力とする所定のアルゴリズムにより第１の認証情報を生成するための第１の認証情報生成手段。(7) 前記第１の認証情報を前記第２の局に送信するための認証情報送信手段。(8) 前記第２の局に設けられ、前記送信されてくるアクセス回数を認証するためのアクセス回数認証手段。(9) 前記第２の局に設けられ、前記送信されてくるアクセス回数と乱数と自局内の前記記憶手段に格納された前記秘密情報とを入力とする所定のアルゴリズムにより第２の認証情報を生成するための第２の認証情報生成

手段。(10)前記第２の局に設けられ、前記第１の認証情報と前記第２の認証情報とを比較することで前記第１の局の正当性を認証するための認証手段。

【００３８】（４）．また、この出願の認証方法の第４の発明によれば、共通の秘密情報をそれぞれの記憶手段に格納している第１の局および第２の局を含む通信システムにおいて、前記第２の局が前記第１の局を認証するに当たり、以下の各処理を含むことを特徴とする。

【００３９】(a) 前記第１の局が、第１の局である旨を示すユーザ情報を前記第２の局に送信する処理。(b) 前記第１の局が、乱数を発生する処理。(c) 前記第１の局が、自局内の前記記憶手段に格納してある前記秘密情報を鍵として前記乱数と前記ユーザ情報とを暗号化することにより認証情報を生成しこれを前記第２の局に送信する処理。(d) 前記第２の局が、自局内の前記記憶手段に格納してある前記秘密情報を鍵として前記送信されてきた認証情報を復号化する処理。(e) 前記第２の局が、前記復号化で得たユーザ情報と前記送信されてきたユーザ情報とを比較すること、および、前記復号化で得た乱数を認証することにより前記第１の局の正当性を認証する処理。

【００４０】この認証方法の第４の発明によれば、第１の局が第２の局にユーザ情報を送信すると認証動作が開始される。しかも、第１の局がユーザ情報および乱数を暗号化して第２の局に送り、第２の局はこれらを復号化しそれにより第１の局を認証する。暗号化および復号化を含むので、その分、認証方法自体が解読されにくいと考えられる。

【００４１】また、この第４発明の場合も、第１の局が第２の局をアクセスするごとに乱数を発生している。この乱数は暗号化された状態で第２の局に送信され、そして第２の局で復号化される。復号化された乱数は認証される。乱数の認証は、例えば、今回復号された乱数が過去の通信の際に復号された乱数履歴に含まれているか否かを調べることにより行なうことが出来る。第３者が通信情報を盗聴してこれを用いて第２の局を攻撃してもこの通信情報から復号される乱数は既に使われた乱数である。すると第２の局は、この攻撃を、第３者によるものと判断することができる。すなわち、復号したユーザ情報のみの認証であると、第３者が通信情報を盗聴してそれを送ってきた場合に第３者が正当とされてしまうが、この第４の発明では復号した乱数をも認証するので、第３者の攻撃を防止することができる。

【００４２】なお、この認証方法の第４の発明において情報を送信する各処理は、それぞれを別々に行なうことを必須とする意味ではない。通信回数を減らす意味から、情報処理に支障がない範囲で、いくつかの送信処理を同時に行ってももちろん良い。例えば、ユーザ情報、乱数および認証情報は同時に送信することができる。

【００４３】この認証方法の第４の発明を実施するため、以下の(1) ～(6) の手段を具えた通信システム（通信システムの第４の発明）を構成するのが好適である。

【００４４】(1) 前記第１の局から前記第２の局に第１の局である旨を示すユーザ情報を送信するためのユーザ情報送信手段。(2) 前記第１の局に設けられ、乱数を発生するための乱数生成手段。(3) 前記第１の局に設けられ、自局内の前記記憶手段に格納してある前記秘密情報を鍵として前記乱数と前記ユーザ情報とを暗号化することにより認証情報を生成するための認証情報生成手段。(4) 前記認証情報を前記第２の局に送信するための認証情報送信手段。(5) 前記第２の局に設けられ、自局内の前記記憶手段に格納してある前記秘密情報を鍵として前記送信されてくる認証情報を復号化するための認証情報復号化手段。(6) 前記第２の局に設けられ、前記復号化により得られたユーザ情報と前記送信されてくるユーザ情報とを比較すること、および、前記復号化により得られた乱数を認証することにより前記第１の局の正当性を認証するための認証手段。

【００４５】（５）．また、この出願の認証方法の第５の発明によれば、共通の秘密情報をそれぞれの記憶手段に格納している第１の局および第２の局を含む通信システムにおいて、前記第２の局が前記第１の局を認証するに当たり、以下の各処理を含むことを特徴とする。

【００４６】(a) 前記第１の局が、第１の局である旨を示すユーザ情報を前記第２の局に送信する処理。(b) 前記第１の局が、第１の乱数および第２の乱数を発生する処理。(c) 前記第１の局が、前記第１の乱数を前記第２の局に送信する処理。(d) 前記第１の局が、前記第２の乱数を鍵として前記ユーザ情報を暗号化して第１の暗号文を生成する処理。(e) 前記第１の局が、自局内の前記記憶手段に格納してある前記秘密情報と前記第１の乱数とを入力とする所定のアルゴリズムにより認証情報を生成するための暗号アルゴリズムの鍵を生成する処理。(f) 前記第１の局が、前記暗号アルゴリズムの鍵を用いて前記第２の乱数と前記第１の暗号文とをさらに暗号化して第２の暗号文を生成しこれを認証情報として前記第２の局に送信する処理。(g) 前記第２の局が、前記送信されてきた第１の乱数を認証する処理。(h) 前記第１の乱数を認証する処理にて前記第１の乱数が正当でないとされた場合に実行され、前記第２の局が前記第１の局を正当でないとする処理。(i)前記第１の乱数を認証する処理にて前記第１の乱数が正当であるとされた場合に実行され、前記第２の局が、自局内の前記記憶手段に格納してある前記秘密情報と前記第１の乱数とを入力とする所定のアルゴリズムにより認証情報を復号化するための鍵を生成し、該鍵を用い前記送信されてきた認証情報を復号化し、該復号化で得たユーザ情報と前記送信されてきたユーザ情報とを比較することにより前記第１の局の正当性を認証する処理。

【００４７】この認証方法の第５の発明によれば、認証

動作において第１の乱数の認証を先ず行なうことができる。第１の乱数の認証は、例えば、上記の第２の発明の説明において説明したように乱数履歴を参照する方法で行なうことが出来る。そして、上記の第２の発明において説明した乱数を認証することの利点が、この第５の発明の場合も同様に得られる。

【００４８】またこの認証方法の第５の発明では、本来の認証動作は次のように行なわれる。第１の局が第１の暗号文を生成しさらにこれを暗号化して認証情報を生成する。第２の局はこの認証情報を復号化しそしてこの復号化で得た情報により第２の局が第１の局を認証する。２重の暗号化を用いているので、上記の第４の発明に比べ認証方法自体がさらに解読されにくいと考えられる。また、認証情報の生成に用いる乱数を第１および第２の乱数としたので、認証情報の生成に用いる乱数が１つの場合より、認証方法自体が解読されにくいと考えられる。

【００４９】なお、この認証方法の第５の発明において情報を送信する各処理は、それぞれを別々に行なうことを必須とする意味ではない。通信回数を減らす意味から、情報処理に支障がない範囲で、いくつかの送信処理を同時に行ってももちろん良い。

【００５０】この認証方法の第５の発明を実施するため、以下の(1) ～(11)の手段を具えた通信システム（通信システムの第５の発明）を構成するのが好適である。

【００５１】(1) 前記第１の局から前記第２の局に対し第１の局である旨を示すユーザ情報を送信するためのユーザ情報送信手段。(2) 前記第１の局に設けられ、第１の乱数および第２の乱数を発生するための乱数生成手段。(3) 前記発生された第１の乱数を前記第２の局に送信するための乱数送信手段。(4) 前記第１の局に設けられ、前記第２の乱数を鍵として前記ユーザ情報を暗号化して第１の暗号文を生成するための暗号文生成手段。(5) 前記第１の局に設けられ、前記第１の乱数と自局内の前記記憶手段に格納してある前記秘密情報とを入力とする所定のアルゴリズムにより認証情報を生成するための暗号アルゴリズムの鍵を生成するための暗号鍵生成手段。(6) 前記第１の局に設けられ、前記暗号アルゴリズムの鍵を用いて前記第２の乱数と前記第１の暗号文とをさらに暗号化して認証情報としての第２の暗号文を生成するための認証情報生成手段。(7) 前記認証情報を前記第２の局に送信するための認証情報送信手段。(8) 前記第２の局に設けられ、前記送信されてくる第１の乱数を認証するための乱数認証手段。(9) 前記第２の局に設けられ、前記送信されてくる第１の乱数と自局内の前記記憶手段に格納してある前記秘密情報とを入力とする所定のアルゴリズムにより前記認証情報を復号化するための鍵を生成するための復号鍵生成手段。(10)前記第２の局に設けられ、前記復号鍵を用いて前記認証情報を復号化するための認証情報復号化手段。(11)前記第２の局に設けられ、前記復号化により得られたユーザ情報と前記送信されてくるユーザ情報とを比較することにより前記第１の局の正当性を認証するための認証手段。

【００５２】(6)．また、この出願の認証方法の第６の発明によれば、共通の秘密情報をそれぞれの記憶手段に格納している第１の局および第２の局を含む通信システムにおいて、前記第２の局が前記第１の局を認証するに当たり、以下の各処理を含むことを特徴とする。

【００５３】(a) 前記第１の局が、第１の局である旨を示すユーザ情報を前記第２の局に送信する処理。(b) 前記第１の局が、乱数を発生する処理。(c) 前記第１の局が、前記第２の局をアクセスした回数を計数する処理。(d) 前記第１の局が、前記乱数を鍵として前記ユーザ情報と前記アクセス回数とを暗号化する処理。(e) 前記第１の局が、自局内の前記記憶手段に格納してある前記秘密情報を鍵として前記暗号化されたユーザ情報と前記アクセス回数とをさらに暗号化してこれを認証情報として前記第２の局に送信する処理。(f) 前記第２の局が、自局内の前記記憶手段に記憶してある前記秘密情報を鍵として前記送信されてきた認証情報を復号化する処理。(g) 前記第２の局が、前記復号化で得たユーザ情報と前記送信されてきたユーザ情報とを比較すること、および、前記復号化で得たアクセス回数を認証することにより前記第１の局の正当性を認証する処理。

【００５４】この認証方法の第６の発明によれば、第１の局が、乱数を鍵とする第１の暗号化と秘密情報を鍵とする第２の暗号化により認証情報を生成し、これを第２の局に送信する。一方、秘密情報自体は第２の局が自局の記憶手段に予め持っている。そのため第２の局は、第１の局から送信されてくる認証情報を、上記の秘密情報および乱数を鍵として復号することができる。そして復号化した情報により第１の局の正当性を認証する。しかも、ユーザ情報およびアクセス回数の両方を暗号化し、かつ、二重の暗号化をしているので、認証方法自体が解読されにくいと考えられる。

【００５５】さらにこの認証方法の第６の発明では、復号したアクセス回数を認証する。アクセス回数の認証は、例えば上述したように、$n'_a+\varepsilon > n_a > n'_a$という不等式関係を満たすか否かを調べることにより行なうことが出来る。第３者が通信情報を盗聴し、これを用いて第２の局を繰り返し攻撃したとしても、これは既に使用されたアクセス回数と同じ値を含む通信情報による攻撃である。すると上記不等式関係を満たさないので、第２の局は、この攻撃を、第３者によるものと判断することができる。

【００５６】なお、この認証方法の第６の発明において情報を送信する各処理は、それぞれを別々に行なうことを必須とする意味ではない。通信回数を減らす意味から、情報処理に支障がない範囲で、いくつかの送信処理を同時に行ってももちろん良い。

【００５７】この認証方法の第６の発明を実施するため、以下の(1)～(8)の手段を具えた通信システム（通信システムの第６の発明）を構成するのが好適である。

【００５８】(1) 前記第１の局から前記第２の局に対し第１の局である旨を示すユーザ情報を送信するためのユーザ情報送信手段。(2) 前記第１の局に設けられ、乱数を発生するための乱数生成手段。(3) 前記第１の局に設けられ、前記第１の局が前記第２の局をアクセスしたアクセス回数を計数するためのアクセス回数計数手段。(4) 前記第１の局に設けられ、前記乱数を鍵として前記ユーザ情報と前記アクセス回数とを暗号化するための暗号化手段。(5) 前記第１の局に設けられ、自局内の前記記憶手段に格納してある前記秘密情報を鍵として前記暗号化されたユーザ情報とアクセス回数とをさらに暗号化することにより認証情報を生成するための認証情報生成手段。(6) 前記認証情報を前記第２の局に送信するための認証情報送信手段。(7) 前記第２の局に設けられ、自局内の前記記憶手段に格納してある前記秘密情報を鍵として前記送信されてくる認証情報を復号化するための認証情報復号化手段。(8) 前記第２の局に設けられ、前記復号化により得られるユーザ情報と前記送信されてくるユーザ情報とを比較すること、および、前記復号化により得られるアクセス回数を認証することにより前記第１の局の正当性を認証するための認証手段。

【００５９】（７）．また、この出願の認証方法の第７の発明によれば、共通の秘密情報をそれぞれの記憶手段に格納している第１の局および第２の局を含む通信システムにおいて、前記第２の局が前記第１の局を認証するに当たり、以下の各処理を含むことを特徴とする。

【００６０】(a) 前記第１の局が、第１の局である旨を示すユーザ情報を前記第２の局に送信する処理。(b) 前記第１の局が、第１の乱数および第２の乱数を発生する処理。(c) 前記第１の局が、該第１の乱数を前記第２の局に送信する処理。(d) 前記第１の局が、前記第２の局をアクセスした回数を計数する処理。(e) 前記第１の局が、前記第２の乱数を鍵として前記ユーザ情報と前記アクセス回数とを暗号化して第１の暗号文を生成する処理。(f) 前記第１の局が、自局内の前記記憶手段に格納してある前記秘密情報と前記第１の乱数とを入力とする所定のアルゴリズムにより認証情報を生成するための暗号アルゴリズムの鍵を生成する処理。(g) 前記第１の局が、前記暗号アルゴリズムの鍵を用いて前記第２の乱数と前記第１の暗号文とをさらに暗号化して第２の暗号文を生成しこれを認証情報として前記第２の局に送信する処理。(h) 前記第２の局が、自局内の前記記憶手段に格納してある前記秘密情報と前記第１の乱数とを入力とする所定のアルゴリズムにより前記認証情報を復号化するための鍵を生成する処理。(i) 前記第２の局が、前記復号化するための鍵を用い前記送信されてきた認証情報を復号化する処理。（ｊ）前記復号化で得たユーザ情報と前記送信されてきたユーザ情報とを比較すること、および、前記復号化で得たアクセス回数を認証することにより前記第１の局の正当性を認証する処理。

【００６１】この認証方法の第７の発明によれば、第１の局が、第２の乱数を鍵とし第１の暗号文を生成する。さらに第１の局が、秘密情報、第１の乱数および所定のアルゴリズムで暗号アルゴリズムの鍵を生成、この鍵を用い第１の暗号文をさらに暗号化して第２の暗号文を生成し、これを認証情報として第２の局に送信する。一方、第２の局には第１の局から第１の乱数が送信されており、かつ、秘密情報自体および所定のアルゴリズム自体は第２の局が予め持っている。そのため、第２の局は、これら第１の乱数、秘密情報および所定のアルゴリズムにより復号化するための鍵を生成できる。生成した復号化するための鍵を用い認証情報を復号化すると第２の乱数すなわち第１の暗号文を生成した際の鍵を復号することができる。この第２の乱数を鍵として用い認証情報を復号化すると、ユーザ情報とアクセス回数とを復号することができる。

【００６２】この認証方法の第７の発明の場合、　：ユーザ情報およびアクセス回数の両方を暗号化し、　：然も二重の暗号化をし、　：然も認証情報生成のための暗号鍵および認証情報復号のための復号鍵それぞれを、秘密情報、第１の乱数および所定のアルゴリズムで生成しているので、上記の第６の発明に比べ、認証方法自体がさらに解読されにくいと考えられる。

【００６３】さらにこの認証方法の第７の発明では、復号されたアクセス回数を認証する。アクセス回数の認証は、例えば上述したように、$n'_a + \varepsilon > n_a > n'_a$という不等式関係を満たすか否かを調べることにより行なうことが出来る。第３者が通信情報を盗聴し、これを用いて第２の局を繰り返し攻撃したとしても、これは既に使用されたアクセス回数を用いた攻撃である。すると上記不等式関係を満たさないので、第２の局は、この攻撃を、第３者によるものと判断することができる。

【００６４】なお、この認証方法の第７の発明において情報を送信する各処理は、それぞれを別々に行なうことを必須とする意味ではない。通信回数を減らす意味から、情報処理に支障がない範囲で、いくつかの送信処理を同時に行ってももちろん良い。

【００６５】この認証方法の第７の発明を実施するため、以下の(1)～(11)の手段を具えた通信システム（通信システムの第７の発明）を構成するのが好適である。

【００６６】(1) 前記第１の局から前記第２の局に対し第１の局である旨を示すユーザ情報を送信するためのユーザ情報送信手段。(2) 前記第１の局に設けられ、第１の乱数および第２の乱数を発生するための乱数生成手段。(3) 前記発生された第１の乱数を前記第２の局に送信するための乱数送信手段。(4) 前記第１の局に設けられ、前記第１の局が前記第２の局をアクセスしたアクセ

ス回数を計数するためのアクセス回数計数手段。(5) 前記第１の局に設けられ、前記第２の乱数を鍵として前記ユーザ情報と前記アクセス回数とを暗号化して第１の暗号文を生成するための暗号文生成手段。(6) 前記第１の局に設けられ、前記第１の乱数と自局内の前記記憶手段に格納してある前記秘密情報とを入力とする所定のアルゴリズムにより認証情報を生成するための暗号アルゴリズムの鍵を生成するための暗号鍵生成手段。(7) 前記第１の局に設けられ、前記暗号アルゴリズムの鍵を用いて前記第２の乱数と前記第１の暗号文とをさらに暗号化して認証情報としての第２の暗号文を生成するための認証情報生成手段。(8) 前記認証情報を前記第２の局に送信するための認証情報送信手段。(9) 前記第２の局に設けられ、前記送信されてくる第１の乱数と自局内の前記記憶手段に格納してある前記秘密情報とを入力とする所定のアルゴリズムにより前記認証情報を復号化するための鍵を生成するための復号鍵生成手段。(10)前記第２の局に設けられ、前記送信されてくる認証情報を前記復号鍵を用い復号化するための認証情報復号化手段。(11)前記第２の局に設けられ、前記復号化により得られるユーザ情報と前記送信されてくるユーザ情報とを比較すること、および、前記復号化により得られるアクセス回数を認証することにより前記第１の局の正当性を認証するための認証手段。

【００６７】上述した認証方法の第１～第７の発明は、第１の局および第２の局間で直接通信を行ない認証を行なう例であった。しかし、通信システムでは、通信を希望する第１の局と第２の局との間に、第１の局の認証を第２の局に代わって行なう信頼できる第３の局が入ったり、中間局が入ることも多い。通信を希望する第１の局または第２の局の負荷を分散する等の目的からである、認証方法の第８～第１０の各発明はその例である。

【００６８】（8）．この出願の認証方法の第８の発明によれば、通信を希望する第１の局および第２の局と、該第２の局に代わって認証をする信頼できる第３の局とを含み、前記第１の局および第３の局は共通の秘密情報をそれぞれの記憶手段に格納している通信システムにおいて、前記第３の局が前記第１の局を実際に認証するに当たり、以下の各処理を含むことを特徴とする。

【００６９】(a) 前記第１の局が、乱数を発生し、該乱数と第１の局である旨を示すユーザ情報とを前記第２の局に送信する処理。(b) 前記第１の局が、前記乱数と自局内の前記記憶手段に格納してある前記秘密情報とを用いて認証情報を生成しこれを前記第２の局に送信する処理。(c) 前記第２の局が、前記第１の局から送信されてきたユーザ情報と乱数と認証情報とを前記第３の局に送信する処理。(d) 前記第３の局が、前記第２の局から送信されてきた認証情報を前記乱数と自局内の前記記憶手段に格納してある前記秘密情報を用いて認証することにより前記第１の局の正当性を認証する処理。(e) 前記第３の局が前記第２の局に認証結果を送信する処理。

【００７０】この認証方法の第８の発明によれば、第２の局は第１の局から送信されてきたユーザ情報と乱数と認証情報とを前記第３の局に送信し、第３の局に第１の局の認証をさせ、その結果を受信することが出来る。第１の局に対し共通の秘密情報を持たない第２の局であっても、第２の局は、第１の局が正当な通信者であるか否かを、第２の局が信頼する第３の局の力を借りて、認証することができる。そのため第２の局は安心して第１の局と通信をおこなうことができる。第２の局が認証動作しない分、第２の局の負荷が軽減される。

【００７１】また認証方法の第８の発明の場合、第１の局で乱数を発生しているので、乱数をユーザ情報と一緒に第２の局に送信することができる。第２の局で乱数を発生した場合（後の認証方法の第９の発明）は、第１の局が認証情報生成に必要な乱数を第２の局が第１の局に送信する専用の処理が必要となるので通信回数が増えてしまう。この点を考えると、第１の局で乱数を発生するのが好ましい。

【００７２】なお、この認証方法の第８の発明において認証情報の生成や認証情報の認証をいかなる方法で行なうかは、任意である。なぜなら、第３の局が含まれた場合に第２の局に変わって第３の局が第１の局を認証できるよう、第１～第３の局間の情報の授受を工夫した点を特徴としているからである（以下の認証方法の第９の発明において同じ。）。ただし好ましくは、上記の認証方法の第２～第７の発明で主張しているそれぞれの認証情報の生成手順、それぞれの認証情報の認証手順のいずれかを用いるのが良い（以下の認証方法の第９の発明において同じ。）。こうすると、第３の局が追加された場合でも、第３者（正当でない通信者）による繰り返し攻撃を防止できるという上記の効果が得られるからである。

【００７３】この認証方法の第８の発明を実施するため、以下の各手段(1) ～(8) を含む通信システム（通信システムの第８の発明）を構成するのが好適である。

【００７４】(1) 前記第１の局から前記第２の局に第１の局である旨を示すユーザ情報を送信するためのユーザ情報送信手段。(2) 前記第１の局に設けられ、乱数を発生するための乱数生成手段。(3) 前記発生された乱数を前記第２の局に送信するための乱数送信手段。(4) 前記第１の局に設けられ、前記乱数と自局内の前記記憶手段に格納された前記秘密情報とを用い認証情報を生成するための認証情報生成手段。(5) 前記認証情報を前記第２の局に送信するための認証情報送信手段。（６）前記第１の局から前記第２の局に送信されてくる前記ユーザ情報、前記乱数および前記認証情報それぞれを前記第３の局に送信するための送信手段。（７）　前記第３の局に設けられ、前記第２の局から送信されてくる前記認証情報を自局内の前記記憶手段に格納してある前記秘密情報を用いて認証することにより前記第１の局の正当性を認

証するための認証手段。(8) 第３の局に設けられ、認証結果を第２の局に送信するための手段。

【００７５】（９）．またこの出願の認証方法の第９の発明によれば、通信を希望する第１の局および第２の局と、該第２の局に代わって認証をする信頼できる第３の局とを含み、前記第１の局および第３の局は共通の秘密情報をそれぞれの記憶手段に格納している通信システムにおいて、前記第３の局が前記第１の局を認証するに当たり、以下の各処理を含むことを特徴とする。

【００７６】(a) 前記第１の局が、第１の局である旨を示すユーザ情報を前記第２の局に送信する処理。(b) 前記第２の局が、前記ユーザ情報を受信すると乱数を発生し該乱数を前記第１の局に送信する処理。(c) 前記第１の局が、前記第２の局から送信されてきた乱数と自局内の前記記憶手段に格納している前記秘密情報とを用いて認証情報を生成しこれを前記第２の局に送信する処理。(d) 前記第２の局が、前記乱数と、前記第１の局から送信されてきたユーザ情報と認証情報とを前記第３の局に送信する処理。(e) 前記第３の局が、前記第２の局から送信されてきたユーザ情報と認証情報とを自局内の前記記憶手段に格納してある前記秘密情報を用いて認証することにより前記第１の局の正当性を認証する処理。(f) 前記第３の局が第２の局に認証結果を送信する処理。

【００７７】この認証方法の第９の発明の場合も第８の発明と同様、第１の局に対し共通の秘密情報を持たない第２の局であっても、第２の局は、第１の局が正当な通信者であるか否かを、第２の局が信頼する第３の局の力を借りて、認証することができる。そのため第２の局は安心して第１の局と通信をおこなうことができる。

【００７８】またこの場合第２の局側が乱数を発生するので、第２の局に対する繰り返し攻撃（正当でない通信）を防止することができる。

【００７９】この認証方法の第９の発明を実施するため、以下の各手段(1) ～(8) を含む通信システム（通信システムの第９の発明）を構成するのが好適である。

【００８０】(1) 前記第１の局から前記第２の局に第１の局である旨を示すユーザ情報を送信するためのユーザ情報送信手段。(2) 前記第２の局に設けられ、前記ユーザ情報を受信すると乱数を発生するための乱数生成手段。(3) 前記発生された乱数を前記第１の局に送信するための乱数送信手段。(4) 前記第１の局に設けられ、前記乱数と自局内の前記記憶手段に格納された前記秘密情報とを用い認証情報を生成するための認証情報生成手段。(5) 前記認証情報を前記第２の局に送信するための認証情報送信手段。(6) 前記乱数と前記第１の局から前記第２の局に送信されてくる前記ユーザ情報および前記認証情報を前記第３の局に送信するための送信手段。(7) 前記第３の局に設けられ、前記第２の局から送信されてくる前記認証情報を自局内の前記記憶手段に格納してある前記秘密情報を用いて認証することにより前記第１の局の正当性を認証するための認証手段。(8) 前記第３の局に設けられ、前記第２の局に認証結果を送信するための手段。

【００８１】（１０）．またこの出願の認証方法の第１０の発明によれば、通信を希望する第１の局および第２の局と、これら局間に介在する中間局とを含み、前記第１の局および第２の局は共通の秘密情報をそれぞれの記憶手段に格納している通信システムにおいて、以下の各処理を含むことを特徴とする。

【００８２】(a) 前記第１の局が、第１の局である旨を示すユーザ情報を前記中間局に送信する処理。(b) 前記中間局が、前記ユーザ情報を受信すると乱数を発生し該乱数を前記第１の局に送信する処理。(c) 前記第１の局が、前記中間局から送信されてきた乱数と自局内の前記記憶手段に格納している前記秘密情報とを用いて認証情報を生成しこれを前記中間局に送信する処理。(d) 前記中間局が、前記乱数と、前記第１の局から送信されてきたユーザ情報と認証情報とを前記第２の局に送信する処理。(e) 前記第２の局が、前記中間局から送信されてきた認証情報を自局内の前記記憶手段に格納している前記秘密情報を用いて認証することにより前記第１の局の正当性を認証する処理。

【００８３】この認証方法の第１０の発明によれば、中間局が第１の局および第２の局の中継処理を行なう。第１の局および第２の局間に秘密情報を共有しない中間局が介在した場合でも、第２の局は、第１の局が正当な通信者であるか否かを、認証することができる。そのため第２の局は安心して第１の局と通信をおこなうことができる。しかも、中間局が乱数発生処理を担うので、その分、第１の局および第２の局の負荷を軽減することができる。

【００８４】なお、この認証方法の第１０の発明において認証情報の生成や認証情報の認証をいかなる方法で行なうかは、任意である。なぜなら、中間局が含まれた場合でも第２の局が第１の局を認証できるよう、第１、第２および中間局の情報の授受を工夫した点を特徴としているからである。ただし好ましくは、上記の認証方法の第２～第７の発明で主張しているそれぞれの認証情報の生成手順、それぞれの認証情報の認証手順のいずれかを用いるのが良いこうすると、中間局が追加された場合でも、第３者（正当でない通信者）による繰り返し攻撃を防止できるという上記の効果が得られるからである。

【００８５】この認証方法の第１０の発明を実施するため、以下の各手段(1) ～(7) を含む通信システム（通信システムの第１０の発明）を構成するのが好適である。

【００８６】(1) 前記第１の局から前記中間局に第１の局である旨を示すユーザ情報を送信するためのユーザ情報送信手段。(2) 前記中間局に設けられ、前記ユーザ情報を受信すると乱数を発生するための乱数生成手段。(3) 前記発生された乱数を前記第１の局に送信するため

の乱数送信手段。(4) 前記第１の局に設けられ、前記送信されてくる乱数と自局内の前記記憶手段に格納してある前記秘密情報とを用いて認証情報を生成するための認証情報生成手段。(5) 前記認証情報を前記中間局に送信するための認証情報送信手段。(6) 前記乱数と前記第１の局から前記中間局に送信されてくる前記ユーザ情報および前記認証情報を前記第２の局に送信するための送信手段。(7) 前記第２の局に設けられ、前記送信されてくる認証情報を自局内の前記記憶手段に格納してある前記秘密情報を用い認証することにより前記第１の局の正当性を認証するための認証手段。

【００８７】（A）．なお認証方法の第１～第３の各発明を実施するに当たり、前記第１の局および第２の局それぞれに、前記所定のアルゴリズムとして用いることができるアルゴリズムを複数種かつ同様に（同じ種類という趣旨）予め用意しておくのが好適である。しかも、前記第１および第２の局のいずれか一方が選択信号を発生し、これに応じ前記第１および第２の局が前記複数種のアルゴリズムの中から１つを選択し、該選択されたアルゴリズムにより前記第１の局は前記第１の認証情報を生成し、前記第２の局は前記第２の認証情報を生成するのが好適である。こうすると、アルゴリズムを変更できる分、認証情報の生成アルゴリズムが増えるので、認証方法が解読されにくくなる。そのため、機密保護能力に優れる通信システムを実現することができる。

【００８８】なお、第１および第２の局それぞれに用意される複数種のアルゴリズムは、例えば両局で共通に番号付けした状態で記憶させたアルゴリズムとするのが良い。そして、番号を指定すると両局で同じアルゴリズムが選択されるようにするのが良い。（以下の（B）、（D）においても同様とするのが良い。）。

【００８９】（B）．また認証方法の第５および第７の各発明を実施するに当たり、前記第１の局および第２の局それぞれに、前記所定のアルゴリズムとして用いることができるアルゴリズムを複数種かつ同様に（同じ種類という趣旨）予め用意しておくのが好適である。しかも、前記第１および第２の局のいずれか一方が選択信号を発生し、これに応じ前記第１および第２の局が前記複数のアルゴリズムの中から１つを選択し、該選択されたアルゴリズムにより、前記第１の局は前記暗号アルゴリズムの鍵を生成し、前記第２の局は前記認証情報を復号化するための鍵を生成するのが好適である。こうすると、アルゴリズムを変更できる分、鍵の種類が増えるため認証情報の生成アルゴリズムが増えるので、認証方法が解読されにくくなる。そのため、機密保護能力に優れる通信システムを実現することができる。

【００９０】（C）．また、認証情報を作成する際に用いる所定のアルゴリズムとして一方向性関数を用いるのが好適である。具体的には、認証方法の第１～第３の発明での第１および第２の認証情報をそれぞれ作成するための所定アルゴリズム、第５および第７の発明で暗号アルゴリズムの鍵および復号化するための鍵それぞれを作成するための所定アルゴリズムとして、一方向性関数を用いるのが好適である。一方向性関数は一方向性ハッシュ関数（one-way hash function）．或は単にハッシュ関数とも呼ばれる。これは、ｘからｆ（ｘ）を計算するのは容易であるが、ｆ（ｘ）からｘを求めるのは極めて困難な関数ｆ（ｘ）である。一方向性関数を用いると、認証情報から秘密情報や乱数等が解読される危険性を低減することができる。

【００９１】（D）．また認証方法の第４～第７の各発明を実施するに当たり、前記第１の局および第２の局それぞれに、前記認証情報を生成する際のアルゴリズムおよび前記認証情報を復号化する際のアルゴリズムとして用いることができる複数種の暗号アルゴリズムを同様（同じ種類という趣旨）に予め用意しておくのが好適である。しかも、前記第１および第２の局のいずれか一方が選択信号を発生し、これに応じ前記第１および第２の局が前記複数の暗号アルゴリズムの中から１つを選択し、該選択された暗号アルゴリズムにより、前記第１の局は前記認証情報を生成する暗号化をし、前記第２の局は前記認証情報を復号化するのが好適である。こうすると、暗号アルゴリズムを変更することができる分、認証情報の生成アルゴリズムが増えるので、認証方法が解読されにくくなる。そのため、機密保護能力に優れる通信システムを実現することができる。

【００９２】（I）．またこの出願の暗号鍵共有方法の第１の発明によれば、　：認証方法の第１～第３の発明のいずれかにより前記第１の局について認証をし、　：該認証により正当とされた場合は前記第１の局および第２の局それぞれで前記乱数および前記秘密情報を入力とする所定の暗号鍵生成アルゴリズムにより共有暗号鍵をそれぞれ生成し、　：これを前記第１および第２の局の共有暗号鍵とすることを特徴とする。

【００９３】この暗号鍵共有方法の第１の発明によれば、第１の局が正当とされると引き続いて共有暗号鍵が生成されるので、第１の局の認証と共有暗号鍵の生成とを連続的に行なうことができる。然も、認証方法で用いた情報である乱数および秘密情報を用い暗号鍵を生成することができる。

【００９４】この暗号鍵共有方法の第１の発明を実施するため、次のように通信システム（通信システムの第１１の発明）を構成するのが好適である。すなわち、通信システムの第１～第３の発明のいずれかの構成に加え、前記第１の局および第２の局それぞれに設けられ、前記認証手段により前記第１の局が正当であるとされた場合に動作し、前記乱数および前記秘密情報を入力とする暗号鍵生成アルゴリズムにより共有暗号鍵を生成する共有暗号鍵生成手段をさらに具えた通信システム。

【００９５】（II）．またこの出願の暗号鍵共有方法の

第２の発明によれば、　：認証方法の第４または第６の発明により前記第１の局について認証をし、　：該認証により正当とされた場合は前記第１の局および第２の局それぞれで前記乱数を入力とする所定の暗号鍵生成アルゴリズムにより共有暗号鍵をそれぞれ生成し、これを前記第１および第２の局の共有暗号鍵とすることを特徴とする。

【００９６】この暗号鍵共有方法の第２の発明によれば、第１の局が正当とされると引き続いて共有暗号鍵が生成されるので、第１の局の認証と共有暗号鍵の生成とを連続的に行なうことができる。然も、認証方法で用いた乱数を用い暗号鍵を生成することができる。

【００９７】この暗号鍵共有方法の第２の発明の発明を実施するため、次のように通信システム（通信システムの第１２の発明）を構成するのが好適である。すなわち、通信システムの第４または第６の発明の構成に加え、前記第１の局および第２の局それぞれに設けられ、前記認証手段により前記第１の局が正当であるとされた場合に動作し、前記乱数を入力とする暗号鍵生成アルゴリズムにより共有暗号鍵を生成する共有暗号鍵生成手段をさらに具えた通信システム。

【００９８】（III）．またこの出願の暗号鍵共有方法の第３の発明によれば、　：認証方法の第５または第７の発明により前記第１の局について認証をし、　：該認証により正当とされた場合は前記第１の局および第２の局それぞれで前記第２の乱数を入力とする所定の暗号鍵生成アルゴリズムにより共有暗号鍵をそれぞれ生成し、　：これを前記第１および第２の局の共有暗号鍵とすることを特徴とする。

【００９９】この暗号鍵共有方法の第３の発明によれば、第１の局が正当とされると引き続いて共有暗号鍵が生成されるので、第１の局の認証と共有暗号鍵の生成とを連続的に行なうことができる。然も、認証方法で用いた情報である第２の乱数を用い暗号鍵を生成することができる。

【０１００】この暗号鍵共有方法の第３の発明の発明を実施するため、次のように通信システム（通信システムの第１３の発明）を構成するのが好適である。すなわち、通信システムの第５または第７の発明の構成に加えて、前記第１の局および第２の局それぞれに設けられ、前記認証手段により前記第１の局が正当であるとされた場合に動作し、前記第２の乱数を入力とする暗号鍵生成アルゴリズムにより共有暗号鍵を生成する共有暗号鍵生成手段をさらに具えた通信システム。

【０１０１】なお、暗号鍵共有方法の第１～第３の発明を実施するに当たり、前記第１の局および第２の局それぞれに、前記所定の暗号鍵生成アルゴリズムとして用いることができるアルゴリズムを複数種かつ同様（同じ種類という趣旨）に予め用意しておく。そして、前記第１および第２の局のいずれか一方が選択信号を発生し、これに応じ前記第１および第２の局が前記複数の暗号鍵生成アルゴリズムの中から１つを選択し、該選択された暗号鍵生成アルゴリズムにより、前記第１の局および第２の局は共有暗号鍵をそれぞれ生成するのが好適である。こうすると、暗号鍵生成アルゴリズムが増えるので、暗号鍵が解読されにくくなる。そのため、機密保護能力に優れる通信システムを実現することができる。

【０１０２】（IV）．またこの出願の暗号鍵共有方法の第４の発明によれば、　：認証方法の第８または第９の発明により前記第１の局について認証をし、　：該認証により正当とされた場合は前記第１の局および第３の局それぞれで共有暗号鍵をそれぞれ生成し、　：前記第３の局は該共有暗号鍵を前記第２の局に送信しこれを前記第２の局は共有暗号鍵とすることを特徴とする。

【０１０３】この暗号鍵共有方法の第４の発明によれば、第１の局が正当とされると引き続いて共有暗号鍵が生成されるので、第１の局の認証と共有暗号鍵の生成とを連続的に行なうことができる。

【０１０４】この暗号鍵共有方法の第４の発明の発明を実施するため、次のように通信システム（通信システムの第１４の発明）を構成するのが好適である。すなわち、通信システムの第８または第９の発明の構成に加えて、前記第１の局および第３の局それぞれに設けられかつ前記認証手段により前記第１の局が正当であるとされた場合に動作する共有暗号鍵生成手段と、前記第３の局で生成された共有暗号鍵を前記第２の局に送信するための共有暗号鍵送信手段とをさらに具えた通信システム。

【０１０５】（V）．またこの出願の暗号鍵共有方法の第５の発明によれば、　：認証方法の第１０の発明により前記第１の局について認証をし、　：該認証により正当とされた場合は前記第１の局および第２の局それぞれで共有暗号鍵をそれぞれ生成し、　：これを前記第１および第２の局の共有暗号鍵とすることを特徴とする。

【０１０６】この暗号鍵共有方法の第５の発明によれば、第１の局が正当とされると引き続いて共有暗号鍵が生成されるので、第１の局の認証と共有暗号鍵の生成とを連続的に行なうことができる。

【０１０７】この暗号鍵共有方法の第５の発明の発明を実施するため、次のように通信システム（通信システムの第１５の発明）を構成するのが好適である。すなわち、通信システムの第１０の発明の構成に加えて、前記第１の局および第２の局それぞれに設けられ、前記認証手段により前記第１の局が正当であるとされた場合に動作する共有暗号鍵生成手段をさらに具えた通信システム。

【０１０８】なお、通信システムの発明を実施するに当たり、特に、以下のように構成するのが好適である。

【０１０９】(i) 通信システムの第２の発明を実施するに当たり、前記乱数認証手段を、前記乱数が正当でないと判断した場合、前記第１の局を正当でないと決定する

手段とするのが好適である。しかも、前記第２の認証情報生成手段および前記認証手段それぞれを、前記乱数認証手段が前記乱数を正当と判断した場合に動作する手段とするのが好適である。こうすると第２の認証情報生成手段および認証手段の必要以上の動作を防止することができるので、通信システムの処理能力の向上、混雑緩和などが図れる。

【０１１０】(ii)通信システムの第３の発明を実施するに当たり、前記アクセス回数認証手段を、前記アクセス回数が正当でないと判断した場合、前記第１の局を正当でないと決定する手段とするのが好適である。しかも、前記第２の認証情報生成手段および前記認証手段それぞれを、前記アクセス回数認証手段が前記アクセス回数を正当と判断した場合に動作する手段とするのが好適である。こうすると第２の認証情報生成手段および認証手段の必要以上の動作を防止することができるので、通信システムの処理能力の向上、混雑緩和などが図れる。

【０１１１】(iii) 通信システムの第５の発明を実施するに当たり、前記第１の乱数認証手段を、前記第１の乱数が正当でないと判断した場合、前記第１の局を正当でないと決定する手段とするのが好適である。しかも、前記復号鍵生成手段、前記認証情報復号化手段および前記認証手段それぞれを、前記第１の乱数認証手段が前記第１の乱数を正当と判断した場合に動作する手段とするのが好適である。こうすると、復号鍵生成手段、認証情報復号化手段および認証手段それぞれの必要以上の動作を防止することができるので、通信システムの処理能力の向上、混雑緩和などが図れる。

【０１１２】

【発明の実施の形態】以下、図面を参照してこの出願の各発明の実施の形態について説明する。しかしながら、説明に用いる各図はこれら発明を理解出来る程度に概略的に示してある。また、各図において同様な構成成分については同一の番号を付して示し、その重複する説明を省略することもある。

【０１１３】なお、この出願でいう第１の局、第２の局、第３の局および中間局それぞれを、コンピュータで構成することができる。また、各局は、通信回線により接続されることにより通信システムを構成する。通信プロトコルは任意のプロトコルとすることができる。また、これら発明でいう、認証情報生成手段、認証手段などの各手段は、コンピュータに備わるＣＰＵ、メモリ、インタフェース回路等およびコンピュータ間を接続している通信回線を組み合わせることにより構成することができる。

【０１１４】１．第１の実施の形態

先ず、認証方法の第１の発明、暗号鍵共有方法の第１の発明、通信システムの第１および第１１の発明それぞれの実施の形態を、併せて説明する。

【０１１５】１－１．通信システムの構成説明

図１は第１の実施の形態の通信システムの構成を説明するための図である。

【０１１６】第１の局１１は、秘密情報格納部１３と、ユーザ情報格納部１５と、送受信インタフェース１７と、所定のアルゴリズムを複数格納する手段１９（関数ｆテーブル１９という）と、第１の認証情報生成手段２１（f_1 演算部２１ともいう）と、共有鍵生成手段２３と、暗号鍵生成アルゴリズムを複数格納する手段２５（関数ｇテーブル２５という）と、共有鍵格納部２７とを具える。

【０１１７】ここで、秘密情報格納部１３は、第１の局および第２の局で共通の秘密情報K_aを記憶するための記憶手段である。この秘密情報格納部１３は、認証情報生成手段２１と共有鍵生成手段２３とに接続してある。認証情報生成手段２１と共有鍵生成手段２３とは、秘密情報を、秘密情報格納部１３から必要に応じ読み出すことができる。

【０１１８】ユーザ情報格納部１５は、第１の局１１についてのユーザ情報I_aを格納するための記憶手段である。このユーザ情報格納部１５は、送受信インターフェース１７と接続してあり、必要に応じ他の局（ここでは第１の局）にユーザ情報を送信することができる。

【０１１９】送受信インタフェース１７は、通信回線（図１の場合は１００）と第２の局４１の送受信インタフェース４５と協力して、この発明でいう各種の送信手段を構成する。

【０１２０】関数ｆテーブル１９は、詳細は後述するが、第１の認証情報生成手段２１が第１の認証情報を生成する際に用いる所定のアルゴリズムを、複数格納するための記憶手段である。この関数ｆテーブル１９は、第１の認証情報生成手段２１と、送受信インタフェース１７とに接続してある。

【０１２１】第１の認証情報生成手段２１は、詳細は後述するが、第１の認証情報を生成するための手段である。この第１の認証情報生成手段２１は、その秘密情報格納部１３から秘密情報を入力し、認証情報を送受信インタフェース１７に出力できるように、構成成分１３、１７と接続してある。

【０１２２】共有鍵生成手段２３は、詳細は後述するが、認証処理にて第１の局が正当とされた場合、共有暗号鍵を生成するための手段である。

【０１２３】関数ｇテーブル２５は、詳細は後述するが、共有暗号鍵生成手段２３が暗号鍵を生成する際に用いる暗号鍵生成アルゴリズムを複数格納するための記憶手段である。この関数ｇテーブル２５は、共有暗号鍵生成手段２３と、送受信インタフェース１７とに接続してある。

【０１２４】共有鍵格納部２７は、共有生成手段２３で生成された共有暗号鍵を格納するための手段である。

【０１２５】一方、第２の局４１は、ユーザ情報・秘密

情報格納部４３と、送受信インタフェース４５と、所定のアルゴリズムを複数格納する手段４７（関数ｆテーブル４７）と、乱数生成手段４９と、第２の認証情報生成手段５１（f_i 演算部５１ともいう）と、共有鍵生成手段５３と、暗号鍵生成アルゴリズムを複数格納する手段５５（関数ｇテーブル５５という）と、共有鍵格納部５７と、認証手段５９とを具えている。

【０１２６】ここで、ユーザ情報・秘密情報格納部４３は、正当な通信者ごとに、ユーザ情報 I_a と秘密情報 K'_a とを格納する記憶手段である。このユーザ情報・秘密情報格納部４３は、送受信インタフェース４５と、第２の認証情報生成手段５１と、共有鍵生成手段５３とにそれぞれ接続してある。第２の局４１は、第１の局１１からユーザ情報 I_a が送信されてくると、このユーザ情報 I_a により、ユーザ情報・秘密情報格納部４３から対応する秘密情報 K'_a を検出することができる。

【０１２７】なお、秘密情報 K_a 、K'_a は同じものであるが、どちらの局側の秘密情報かを区別するために、K_a 、K'_a と示している。

【０１２８】送受信インタフェース４５は、第１の局１１側の送受信インタフェース同様、この発明でいう各種の送信手段の構成成分の１つである。

【０１２９】関数ｆテーブル４７は、詳細は後述するが、第２の認証情報生成手段５１が第２の認証情報を生成する際に用いる所定のアルゴリズムを複数格納するための記憶手段である。この関数ｆテーブル５１は、第２の認証情報生成手段５１と、送受信インタフェース４５とに接続してある。

【０１３０】乱数生成手段４９は、第１の局１１からユーザ情報 I_a を受信すると，乱数ｒを発生するための手段である。この乱数生成手段４９は、送受信インタフェース４５と、第２の認証情報生成手段５１と、共有鍵生成手段５３とにそれぞれ接続している。しかも発生された乱数ｒは第１の局１１側の、第１の認証情報生成手段２１と、共有鍵生成手段２３にも送信される。なお、乱数生成手段４９を第１の局１１側に設け、第２の局４１に第１の局１１から乱数ｒを送信するようにしても良い。

【０１３１】第２の認証情報生成手段５１は、詳細は後述するが、第２の認証情報を生成するための手段である。この第２の認証情報生成手段５１は、その出力を認証手段５９に接続してある。

【０１３２】共有鍵生成手段５３は、詳細は後述するが、認証処理にて第１の局が正当とされた場合、共有暗号鍵を生成するための手段である。

【０１３３】関数ｇテーブル５５は、詳細は後述するが、共有暗号鍵生成手段５３が暗号鍵を生成する際に用いる暗号鍵生成アルゴリズムを複数格納するための記憶手段である。この関数ｇテーブル５５は、共有暗号鍵生成手段５３と、送受信インタフェース４５とに接続してある。

【０１３４】共有鍵格納部５７は、共有生成手段２３で生成された共有暗号鍵を格納するための手段である。

【０１３５】認証手段５９は、第１の認証情報と第２の認証情報とを比較してその結果に応じ第１の局が正当であるか否かを認証する手段である。ここでは認証手段５９を第１の認証情報と第２の認証情報とを比較する比較部で構成してある。

【０１３６】次に、いままでの説明で説明を簡単に済ませた構成成分について詳細に説明する。

【０１３７】まず、第１の認証情報生成手段２１は、秘密情報 K_a と乱数ｒと所定のアルゴリズムとから第１の認証情報を生成する。第２の認証情報生成手段５１は、秘密情報 K'_a（＝K_a）と乱数ｒと所定のアルゴリズムとから第２の認証情報を生成する。

【０１３８】この実施の形態では第１および第２の認証情報を生成するときに用いる所定のアルゴリズムとして、一方向性関数 f_i を用いる。したがって、第１の認証情報生成手段２１は、一方向性関数 f_i と、乱数ｒと、秘密情報 K_a とを用い第１の認証情報 f_i（ｒ，K_a）を生成する。一方、第２の認証情報生成手段５１は、一方向性関数 f_i と、乱数ｒと、秘密情報 K'_a とを用い第２の認証情報 f_i（ｒ，K'_a）を生成する。

【０１３９】しかもこの実施の形態では、一方向性関数 f_i は、第１の認証情報生成手段２１については関数ｆテーブル１９から、また、第２の認証情報生成手段５１については関数ｆテーブル４７から、それぞれ入力される構成としてある。

【０１４０】なお一方向性関数は、一方向性ハッシュ関数（one-way hash function）、或は単にハッシュ関数とも呼ばれる。一方向性関数とは簡単にいうと、ｘからｆ（ｘ）を計算するのは容易であるが、ｆ（ｘ）からｘを求めるのは極めて困難な関数ｆ（ｘ）である。

【０１４１】一方向性関数の具体例として、ＭＤ５（R. Rivest:The MD5 Message-Digest Algorithm, Networking Group, RFC 1321, 1992）やＳＨＡ（National Institute ofStandards and Technology:Secure Hash Standard, FIPS PUB 180-1, 1995）などを挙げることができる。

【０１４２】また関数ｆテーブル１９、４７それぞれには、複数の一方向性関数 f_i を同じ種類それぞれ格納してある。しかも、格納した各関数に、両局で共通の番号を付してある。各関数ｆテーブル１９、４７に対し同じ番号ｉ（例えばｉ＝１，２，３，・・・のいずれか）を入力することで、各関数ｆテーブル１９、４７から、同じ一方向性関数を選択することができる。

【０１４３】なお、一方向性関数選択番号ｉは、例えば第１の局１１の通信開始信号に応じて第１の局１１または第２の局４１が、例えば乱数を用いたり、予め用意されたプログラムに従い、生成する。第１の局１１および第２の局４１のいずが番号ｉを生成するかは、通信シス

テムの設計に応じ決めるのが良い。この第１の実施の形態の場合は、第２の局４１側で番号ｉを生成している。

【０１４４】一方向性関数を上記のＭＤ５等とした場合、関数ｆテーブル１９、４７それぞれを、例えば、１．f_1：ＭＤ５　２．f_2：ＳＨＡ　３．f_3：ＨＭＡＣ－ＭＤ５　４．f_4 ＨＭＡＣ－ＳＨＡ　５．・・・のようにすることができる。

【０１４５】なお、関数ｆテーブルを用いることなく、第１の局１１および第２の局４１に共通な１つの一方向性関数を、認証情報生成のための所定のアルゴリズムとする場合があっても良い。

【０１４６】また関数ｇテーブル２５、５５それぞれには、共有暗号鍵の生成に用いることができる暗号鍵生成アルゴリズムg_j（一方向性関数とは限らない。）を、同じ種類それぞれ格納してある。しかも、格納した各関数に、両局で共通の番号を付してある。各関数ｇテーブル２５、５５に対し同じ番号ｊ（例えばｊ＝１，２，３，・・・のいずれか）を入力することで、各関数ｇテーブル２５、５５から、同じ暗号鍵生成アルゴリズムを選択することができる。

【０１４７】なお、関数ｇテーブル２５、５５から関数を選択するための選択番号ｊは、例えば第１の局１１の通信開始信号に応じて第１の局１１または第２の局４１に備わる例えばＣＰＵ（図示せず）が、乱数を用いたり、予め用意されたプログラムに従い、生成する。この第１の実施の形態では第２の局４１側が選択番号ｊを生成することとしている。

【０１４８】ここで関数ｇテーブル２５、５５それぞれに格納する関数g_jは、通信局間相互で決める任意好適なものとできる。例えばｇ（ｘ）＝Ｘやｇ（ｘ）＝S^n（ｘ）（左ｎ－巡回シフト）などを挙げることができる。その場合、関数ｇテーブルとして、１．g_1（ｘ）＝Ｘ　２．g_2（ｘ）＝S^n（ｘ）（左ｎ－巡回シフト）　３．・・・等が考えられる。

【０１４９】なお、関数ｇテーブルを用いることなく、第１の局１１および第２の局４１に共通な１つのアルゴリズムを、共有暗号鍵生成のための所定のアルゴリズムとする場合があっても良い。

【０１５０】また共有鍵生成手段２３は、第１の局１１が正当であるとされた場合、認証方法で用いた情報のうちの１または複数と、関数ｇテーブル２５から選択された関数g_jとにより、共有暗号鍵化を生成する。この第１の実施の形態では、乱数ｒと、秘密情報K_aと、関数ｇテーブル２５から選択された関数g_jとにより、共有暗号鍵化g_j（ｒ，K_a）を生成する。生成された共有暗号鍵g_j（ｒ，K_a）を、共有鍵格納部２７は内部に格納する。

【０１５１】また、共有鍵生成手段５３は、第１の局１１が正当であるとされた場合、認証方法で用いた情報のうちの１または複数と、関数ｇテーブル５５から選択された関数g_jとにより、共有暗号鍵化を生成する。この第１の実施の形態では乱数ｒと、秘密情報K'_aと、関数ｇテーブル５５から選択された関数g_jとにより、共有暗号鍵化g_j（ｒ，K'_a）を生成する。生成された共有暗号鍵g_j（ｒ，K'_a）を、共有鍵格納部５７は内部に格納する。

【０１５２】なお以下の他の実施の形態では、共有暗号鍵の生成のために用いる情報が、乱数ｒや秘密情報K_aでなく、乱数ｒのみの場合や、第２の乱数r_2のみの場合等がある。しかし、以下の実施の形態の各説明図では共有鍵生成手段には共通に２３、５３という番号を付している。

【０１５３】１－２．動作の説明

次に、第１の実施の形態の通信システムの動作を説明する。これにより、認証方法および共有暗号鍵の生成方法の処理手順を説明する。この説明を図１に加えて図２を参照して行なう。図２は処理の流れを示した図である。

【０１５４】第１の局１１は、ユーザ情報I_aを第２の局４１に送信する（図２の通信１０１）。

【０１５５】ユーザ情報I_aを受信した第２の局４１は、乱数生成手段４９を用いて乱数ｒを生成し、これを第１の局に返信する（図２の通信１０２）。なお、認証情報の生成に使う一方向性関数f_iを指定する場合、第２の局４１は、乱数ｒと共に関数番号ｉも第１の局１１に送信する。また一方向性関数を指定しないときは事前に決められた関数を両局１１、４１は使うことになる。

【０１５６】次に、第１の局１１は、乱数ｒと自分のもつ秘密情報K_aとを使い、かつ、指定された或は事前に決められた一方向性関数f_iを用いて、第１の認証情報f_i（ｒ，K_a）を計算し（図２の処理１１１）、これを第２の局４１の認証手段５９に送信する（図２の通信１０３）。

【０１５７】第１の認証情報f_i（ｒ，K_a）を受信した第２の局４１は、次に、ユーザ情報I_aに対応する秘密情報K'_aを、ユーザ情報・秘密情報格納部４３から見つけ出す。さらに第２の局４１は、乱数ｒと秘密情報K'_aとを使い、かつ、番号ｉに対応する一方向性関数f_iを用いて、第２の認証情報f_i（ｒ，K'_a）を計算し（図２の処理１１２）、これを認証手段（比較部）５９に入力する。

【０１５８】次に、認証手段５９は、第１の認証情報f_i（ｒ，K_a）と、第２の認証情報f_i（ｒ，K'_a）とを比較する（図２の処理１１３）。この比較で両者が等しければ、第２の局４１は第１の局１１の正当性を認め、そして通信許可信号”ＯＫ”と共有暗号鍵生成のための関数g_iの番号ｊとを、第１の局１１に送信する（図２の通信１０４）。また、第２の局４１の共有鍵生成手段５３は、共有暗号鍵を

$K_{12}=g_j$（ｒ，K'_a）

のように生成する（図２の処理１１４）。

【０１５９】一方、通信許可信号”ＯＫ”を受信した第１の局１１は、共有鍵生成手段２３を用いて共有暗号鍵を

$K_{12}=g_j\ (r,\ K_a)$

のように生成する（図２の処理１１５）。

【０１６０】この第１の実施の形態によれば、ユーザ情報と第三者に知られていない秘密情報とを用いて、第２の局が第１の局の正当性を認証することができる。しかも、認証の際に用いた情報である乱数および秘密情報をそのまま用いて第１の局および第２の局の間に暗号鍵の共有を実現している。しかも、第１の局の認証処理と、第１の局および第２の局の間の共有暗号鍵の生成処理とを連続的に行なうことができる。

【０１６１】２．第２の実施の形態

次に、認証方法の第２の発明、暗号鍵共有方法の第１の発明、通信システムの第２および第１１の発明それぞれの実施の形態を、併せて説明する。

【０１６２】２－１．通信システムの構成説明

図３は第２の実施の形態の通信システムの構成を説明する図である。

【０１６３】この第２の実施の形態の第１の実施の形態との主な相違点は、　：第２の局４１側に設けていた乱数生成手段４９を省略し、その代わりに第１の局１１側に乱数生成手段２９を設けた点と、　：第２の局４１内に乱数認証手段６１を設けた点と、　：第２の局４１にユーザ情報・乱数履歴情報・秘密情報格納部６３を設けた点である。

【０１６４】ここで、乱数生成手段２９は、第１の認証情報生成手段２１と、共有鍵生成手段２３と、送受信インターフェース１７とに接続してある。また発生された乱数ｒは第２の局４１側の、第２の認証情報生成手段５１と、共有鍵生成手段５３にも送信される。

【０１６５】ユーザ情報・乱数履歴情報・秘密情報格納部６３は、ユーザ情報I_aおよび秘密情報K'_aを記憶していると共に、正当な通信者ごとの通信で使用された乱数ｒを通信の度に記憶する（乱数履歴を記憶する）記憶手段である。このユーザ情報・乱数履歴情報・秘密情報格納部６３は、送受信インターフェース１７と、乱数認証手段６１と、第１の認証情報生成手段５１とに接続してある。

【０１６６】また、乱数認証手段６１は、第１の局から送信されてくる乱数ｒが、過去に送信されてきた乱数であるか否かを、通信が行なわれる度に、ユーザ情報・乱数履歴情報・秘密情報格納部６３を検索して判定する手段である。この乱数認証手段６１をここでは比較部６１で構成してある。この乱数認証手段６１は、送受信インターフェース４５とユーザ情報・乱数履歴情報・秘密情報格納部６３とに接続してある。

【０１６７】この第２の実施の形態の通信システムでは、乱数生成手段２９、乱数認証手段６１およびユーザ情報・乱数履歴情報・秘密情報格納部６３以外の構成は、第１の実施の形態と同じとしてある。

【０１６８】２－２．動作の説明

次に、第２の実施の形態の通信システムの動作を説明する。これにより、認証方法および共有暗号鍵の生成方法の処理手順を説明する。この説明を図３に加えて図４を参照して行なう。図４は処理の流れを示した図である。

【０１６９】第１の局１１の乱数生成手段２９は通信のごとに異なる乱数ｒを生成する。第１の局１１の第１の認証情報生成部２１は、この乱数ｒと、秘密情報K_aと、一方向性関数f_iとにより、第１の認証情報f_i（ｒ，K_a）を計算する（図４の処理２１１）。

【０１７０】次に、第１の局１１は、第２の局４１に、ユーザ情報I_aと、乱数ｒと、一方向性関数番号ｉと、第１の認証情報f_i（ｒ，K_a）とを送信する（図４の通信２０１）。

【０１７１】次に、第２の局４１は、ユーザ情報I_aを用いて、第１の局１１についての乱数履歴と秘密情報K'_aとを、ユーザ情報・乱数履歴情報・秘密情報格納部６３から見つけ出す。次にまず、第２の局４１の乱数認証手段６１が、乱数履歴を調べて（図４の処理２１２）、もし受信した乱数ｒが乱数履歴に入っているならば第１の局１１の正当性を認めない。

【０１７２】乱数履歴を調べた結果、第１の局１１の正当性を認めないこととなった場合は、第２の局４１は認証動作を中止する。そして第２の局４１は、通信を終了させたり、第１の局１１にエラーメッセージを出す等任意好適な処置をとる。

【０１７３】一方、今回送信されてきた乱数が乱数履歴に含まれていなかった場合は、第２の局４１の第２の認証情報生成手段５１が、この乱数ｒと秘密情報K'_aと一方向性関数f_iとを用いて第２の認証認証情報f_i（ｒ，K'_a）を計算する（図４の処理２１３）。また、第２の局４１は今回送信されてきた乱数ｒを、ユーザ情報・乱数履歴情報・秘密情報格納部６３に、乱数履歴情報として追加する。

【０１７４】次に、第２の局４１の認証手段５９は、第１の認証情報f_i（ｒ，K_a）と第２の認証情報f_i（ｒ，K'_a）とを比較する（図４の処理２１４）。この比較において両者が等しければ、第２の局４１は、第１の局１１の正当性を認め、通信許可信号”ＯＫ”と共有暗号鍵生成のための関数g_jの番号ｊとを、第１の局１１に送信する（図４の通信２０２）。また、第２の局４１の共有鍵生成手段５３は、共有暗号鍵を

$K_{12}=g_j\ (r,\ K'_a)$

のように生成する（図４の処理２１５）。

【０１７５】一方、通信許可信号”ＯＫ”を受信した第１の局１１は、共有鍵生成手段２３を用い共有暗号鍵を

$K_{12}=g_j\ (r,\ K_a)$

のように生成する（図４の処理２１６）。

【０１７６】この第２の実施の形態によれば、ユーザ情報と第三者に知られていない秘密情報とを用いて、第２の局が第１の局の正当性を認証することができる。しかも、認証の際に用いた情報である乱数および秘密情報をそのまま用いて第１の局および第２の局の間に暗号鍵の共有を実現している。しかも、第１の局の認証処理と、第１の局および第２の局の間の共有暗号鍵の生成処理とを連続的に行なうことができる。

【０１７７】また送信されてきた乱数が乱数履歴に含まれるか否かで、第１の局の正当性を判断することができる。そのため、正当でない通信者による繰り返し攻撃を止することができる。

【０１７８】また、第１の局が正当であることの認証は、第１の実施の形態と同様に行なうことができるので、安全性も確保できる。

【０１７９】またこの第２の実施の形態の方が、第１の実施の形態の場合に比べ、通信回数を少なくすることができる。

【０１８０】３．第３の実施の形態

次に、認証方法の第３の発明、暗号鍵共有方法の第１の発明、通信システムの第３および第１１の発明それぞれの実施の形態を、併せて説明する。

【０１８１】３－１．通信システムの構成説明

図５は第３の実施の形態の通信システムの構成を説明する図である。

【０１８２】この第３の実施の形態の第１の実施の形態との主な相違点は、　：第２の局４１側に設けていた乱数生成手段４９を省略し、第２の実施の形態と同じく第１の局１１側に乱数生成手段２９を設けた点と、　：第２の局４１内にアクセス回数認証手段６５を設けた点と、　：第２の局４１にユーザ情報・アクセス回数・秘密情報格納部６７を設けた点と、　：第１の局１１に第１の局１１が第２の局４１をアクセスするごとにアクセス回数を計数するアクセス回数計数手段３１を設けた点である。

【０１８３】なお、乱数生成手段を第２の局４１側に設ける場合があっても良い。しかし、第１の局１１側に乱数生成手段を設けると、乱数とユーザ情報とを一緒に第２の局４１に送信出来るので、通信回数を少なくすることができる。

【０１８４】ここでアクセス回数計数手段３１は、第１の局１１が第２の局４１をアクセスする度にアクセス回数を計数する手段である。このアクセス回数計数手段３１は、送受信インタフェース１７と、第１の認証情報生成手段２１とに接続してある。

【０１８５】このアクセス回数計数手段３１は、第１の局１１が第２の局４１をアクセスするごとに例えば単調増加するカウンタにより構成することができる。なお、アクセス回数計数手段３１で計数されたアクセス回数n_aは、送受信インタフェース１７、４５と通信回線１００とを介して、第２の局４１のアクセス回数認証手段６５に送信される。

【０１８６】またアクセス回数認証手段６５は、第１の局１１から送信されてくるアクセス回数n_aが、第１の局からの過去のアクセス回数に対し正当な範囲にあるか否かを判定することでアクセス回数を認証する手段である。このアクセス回数認証手段６５は、ユーザ情報・アクセス回数・秘密情報格納部６３と、送受信インターフェース４５とに接続してある。

【０１８７】このアクセス回数認証手段６５は、この実施の形態では、第１の局１１から今回送信されてきたアクセス回数をn_a、ユーザ情報・アクセス回数・秘密情報格納部６７に格納されている第１の局の前回の通信までのアクセス回数をn'_a、通信ミスを許容する許容値をε（例えば５程度）としたとき、n_aについて$n'_a + \varepsilon > n_a > n'_a$という不等式関係が成立するか否かをチェックする比較部としてある。

【０１８８】またユーザ情報・アクセス回数・秘密情報格納部６３は、ユーザ情報I_aおよび秘密情報K'_aを記憶していると共に、アクセス回数認証手段６５が正当と認証したアクセス回数n_aをその都度アクセス回数n'_aとして更新記憶する記憶手段である。このユーザ情報・アクセス回数・秘密情報格納部６３は、送受信インターフェース４５と、第２の認証情報生成手段５１と、共有鍵生成手段５３と、アクセス回数認証手段６５とに接続してある。

【０１８９】この第３の実施の形態の通信システムでは、乱数生成手段２９、アクセス回数計数手段３１、アクセス回数認証手段６５およびユーザ情報・アクセス回数・秘密情報格納部６７以外の構成は、第１の実施の形態と同じとしてある。ただし、第１の認証情報生成手段２１と第２の認証情報生成手段５１は、この場合、乱数rと、アクセス回数n_a（n'_a）と、秘密情報K_a（K'_a）と、一方向性関数f_iとにより、第１および第２の認証情報を生成する構成としてある。

【０１９０】３－２．動作の説明

次に、第３の実施の形態の通信システムの動作を説明する。これにより、認証方法および共有暗号鍵の生成方法の処理手順を説明する。この説明を図５に加えて図６を参照して行なう。図６は処理の流れを示した図である。

【０１９１】第１の局１１の乱数生成手段２９は、通信の際乱数rを生成する。第１の局１１のアクセス回数計数手段３１は、計数値すなわちアクセス回数n_aを１増加させ、$n_a = n_a + 1$とする。第１の局１１の第１の認証情報生成部２１は、乱数rと、秘密情報K_aと、アクセス回数n_aとを使い、かつ、一方向性関数f_iを用いて、第１の認証情報$f_i(r, n_a, K_a)$を計算する（図６の処理３１１）。

【０１９２】次に、第１の局１１は、第２の局４１に、ユーザ情報I_aと、乱数rと、一方向性関数番号iと、

アクセス回数n_aと、第１の認証情報f_i（r，n_a，K_a）とを送信する（図６の通信３０１）。

【０１９３】次に、第２の局４１は、ユーザ情報I_aを用いて、ユーザ情報・アクセス回数・秘密情報格納部６７から、第１の局１１についてのアクセス回数n'_aと秘密情報K'_aとを見つけ出す。次にまず、第２の局４１のアクセス回数認証手段６５が、今回受信したアクセス回数n_aについて、$n'_a+\varepsilon > n_a > n'_a$という不等式関係が成立するか否かを調べる（図６の処理３１２）。成立しなければ、第１の局１１の正当性を認めない。

【０１９４】第１の局１１の正当性を認めないこととなった場合は、第２の局４１は認証動作を中止する。また第２の局４１は、通信を終了させたり、第１の局１１にエラーメッセージを出す等任意好適な処置をとる。

【０１９５】一方、上記の不等式関係が成立する場合は、ユーザ情報・アクセス回数・秘密情報格納部６７に記憶してあるアクセス回数n'_aを今回送信されてきたアクセス回数n_aに変更する（図６の処理３１３）。そして、第２の局４１の第３の認証情報生成手段５１は、乱数r と、アクセス回数n'_a（$=n_a$）と、秘密情報K'_aと、一方向性関数f_iとにより、第２の認証情報f_i（r，n'_a，K'_a）を計算する（図６の処理３１４）。

【０１９６】次に、第２の局４１の認証手段５９は、第１の認証情報f_i（r，n_a，K_a）と第２の認証情報f_i（r，n'_a，K'_a）とを比較する（図６の処理３１５）。この比較において両者が等しければ、第２の局４１は、第１の局１１の正当性を認め、通信許可信号”ＯＫ”と共有暗号鍵生成のための関数g_jの番号ｊとを、第１の局１１に送信する（図６の通信３０２）。また、第２の局４１の共有鍵生成手段５３は、共有暗号鍵を

$K_{12}=g_j$（r，K'_a）

のように生成する（図６の処理３１６）。

【０１９７】一方、通信許可信号”ＯＫ”を受信した第１の局１１は、共有鍵生成手段２３を用い共有暗号鍵を

$K_{12}=g_j$（r，K_a）

のように生成する（図６の処理３１７）。

【０１９８】この第３の実施の形態によれば、ユーザ情報と第三者に知られていない秘密情報とを用いて、第２の局が第１の局の正当性を認証することができる。しかも、認証の際に用いた情報である乱数および秘密情報をそのまま用いて第１の局および第２の局の間に暗号鍵の共有を実現している。しかも、第１の局の認証処理と、第１の局および第２の局の間の共有暗号鍵の生成処理とを連続的に行なうことができる。

【０１９９】また送信されてきたアクセス回数が所定の不等式関係を満たすか否かにより、第１の局の正当性を判断することができる。そのため、正当でない通信者による攻撃を防止することができる。

【０２００】また、第１の局が正当であることの認証は、第１の実施の形態と同様に行なうことができるので、安全性も確保できる。

【０２０１】またこの第２の実施の形態の方が、第１の実施の形態の場合に比べ、通信回数を少なくすることができる。

【０２０２】また、この第３の実施の形態では、第２の局４１はアクセス回数を記憶するので、乱数履歴を記憶する場合に比べ第２の局４１でのメモリを節約することができる。

【０２０３】４．第４の実施の形態

次に、認証方法の第４の発明、暗号鍵共有方法の第２の発明、通信システムの第４および第１２の発明それぞれの実施の形態を、併せて説明する。

【０２０４】４－１．通信システムの構成説明

図７は第４の実施の形態の通信システムの構成を説明する図である。

【０２０５】上述の第１～第３の実施の形態では認証情報の生成を一方向性関数を用いて行なっていた。この第４の実施の形態では、認証情報を生成する際に、一方向性関数の代わりに、暗号化アルゴリズムを用いる。

【０２０６】この第４の実施の形態の第１の実施の形態との主な相違点は、　：第２の局４１側に設けていた乱数生成手段４９を省略し、第２の実施の形態と同じく第１の局１１側に乱数生成手段２９を設けた点と、　：第１の局１１に、秘密情報を鍵として乱数およびユーザ情報を暗号化することにより認証情報を生成する認証情報生成手段３３（暗号化部３３ともいう）を設けた点と、　：第１の局１１に上記暗号化のためのアルゴリズムを複数記憶している記憶手段３５（アルゴリズムＥテーブル３５ともいう）を設けた点と、　：第２の局に認証情報を復号する認証情報復号手段６９（復号化部６９ともいう）を設けた点と、　：第２の局４１にアルゴリズムＥテーブル３５に対応するアルゴリズムＥテーブル７１を設けた点と、　：第２の実施の形態と同じく第２の局４１にユーザ情報・乱数履歴・秘密情報格納部６３を設けた点と、　：第２の局４１に、第１の実施の形態で設けていた認証手段５９の代わりに、乱数履歴およびユーザ情報に基づいて第１の局の正当性を認証する認証手段７３を設けた点である。

【０２０７】ここで、アルゴリズムＥテーブル３５、７１それぞれでは、格納された複数の暗号化アルゴリズムに、両局１１、４１で共通の番号を付してある。各アルゴリズムＥテーブル３５、７１に対し同じ番号ｑを入力することで、各アルゴリズムＥテーブル３５、７１から、同じ暗号化アルゴリズムE_qを選択することができる。アルゴリズムＥテーブル３５は、送受信インタフェース１７と認証情報生成手段としての暗号化部３３とに接続してある。また、アルゴリズムＥテーブル７１は、送受信インタフェーズ４５と認証情報復号化手段としての復号化部６９とに接続してある。

【０２０８】なお、暗号化アルゴリズムの選択番号ｑ

は、例えば第１の局１１の通信開始信号に応じて第１の局１１または第２の局４１が、例えば乱数を用いたり、予め用意されたプログラムに従い、生成する。第１の局１１および第２の局４１のいずが番号ｑを生成するかは、設計に応じ決めるのが良い。

【０２０９】ここで、暗号化アルゴリズムの具体例としては、たとえば、ＤＥＳ　ＣＢＣやＭＩＳＴＹやＴｒｉｐｌｅ　ＤＥＳ－ＥＤＥ－ＣＢＣなどを挙げることができる。その場合、アルゴリズムＥテーブル３５、７１それぞれは、１．E_1：ＤＥＳ　ＣＢＣ　２．E_2：ＭＩＳＴＹ　３．E_3：ＴｒｉｐｌｅＤＥＳ－ＥＤＥ－ＣＢＣ　４．・・・のようにすることができる。

【０２１０】なお、アルゴリズムＥテーブル３５、７１を用いることなく、第１の局１１および第２の局４１に共通な１つの暗号化アルゴリズムを、認証情報生成のための所定のアルゴリズムとする場合があっても良い。

【０２１１】また、認証情報生成手段３３としての暗号化部３３は、アルゴリズムＥテーブル３５から選択された暗号化アルゴリズムE_qを用い、乱数ｒとユーザ情報I_aとを、秘密情報K_aを鍵として暗号化し、認証情報としてのE_q｛K_a，（ｒ｜E_q｛ｒ，I_a｝）｝を生成する手段である（詳細は後述する）。認証情報生成手段３３の出力を送受信インターフェース１７に接続してある。

【０２１２】また、認証情報復号手段６９としての復号化部６９は、第１の局１１の認証情報生成手段３３から送信されてきた認証情報としてのE_q｛K_a，（ｒ｜E_q｛ｒ，I_a｝）｝から、乱数ｒとユーザ情報I_aとを復号する手段である（詳細は後述する）。認証情報復号手段６９の出力を認証手段７３と接続してある。

【０２１３】また、認証手段７３は、認証情報復号手段６９で復号されたユーザ情報と第１の局から送信されてくるユーザ情報とを比較する比較部７３ａと、認証情報復号手段６９で復号された乱数を乱数履歴と比較する比較部７３ｂとで構成してある。この認証手段７３は、２つの比較部７３ａ、７３ｂでそれぞれ比較結果が合格となった場合に、第１の局を正当と認証する手段である。

【０２１４】この第４の実施の形態の通信システムでは、乱数生成手段２９、認証情報生成手段３３、アルゴリズムＥテーブル３５、７１、認証情報復号手段６９、ユーザ情報・乱数履歴・秘密情報格納部６３および認証手段７３以外の構成は、第１の実施の形態と同じとしてある。

【０２１５】４－２．動作の説明

次に、第３の実施の形態の通信システムの動作を説明する。これにより、認証方法および共有暗号鍵の生成方法の処理手順を説明する。この説明を図７に加えて図８を参照して行なう。図８は処理の流れを示した図である。

【０２１６】第１の局１１の乱数生成手段２９は、通信の際乱数ｒを生成する。第１の局１１の認証情報生成手段３３は、秘密情報K_aを鍵に乱数ｒとユーザ情報とを暗号化して認証情報を生成する。この場合は次のように暗号化をする。先ず、乱数ｒを鍵としてにユーザ情報I_aを暗号化してE_q｛ｒ，I_a｝という暗号文を得る。ただしE_qはアルゴリズムＥテーブル３５から選択されたｑ番目の暗号化アルゴリズムである。次に、秘密情報K_aを鍵として乱数ｒと上記の暗号文E_q｛ｒ，I_a｝をさらに暗号化して、認証情報としてのE_q｛K_a，（ｒ｜E_q｛ｒ，I_a｝）｝を得る（図８の処理４１１）。ただし、記号”｜”は連結を意味し、Ｅ｛Ｋ，Ｘ｝の表記は暗号鍵Ｋを用いてＸを暗号化したものを意味する。

【０２１７】次に、第１の局１１は、第２の局４１に、ユーザ情報I_aと、暗号化アルゴリズム選択番号ｑと、認証情報としてのE_q｛K_a，（ｒ｜E_q｛ｒ，I_a｝）｝とを送信する（図８の通信４０１）。

【０２１８】認証情報としてのE_q｛K_a，（ｒ｜E_q｛ｒ，I_a｝）｝を受信した第２の局４１は、ユーザ情報・乱数履歴・秘密情報格納部６３から、ユーザ情報I_aを用い第１の局についての秘密情報K'_a（K_a）と乱数履歴とを見つけ出す。さらに第２の局４１は認証情報復号化手段６９を用いて、秘密情報K'_aを鍵として、認証情報である暗号文E_q｛K_a，（ｒ｜E_q｛ｒ，I_a｝）｝を復号してすなわち解読して、乱数ｒを得る。さらに、ｒを鍵にE_q｛ｒ，I_a｝を復号してすなわち解読して、I_aを得る（図８の処理４１２）。

【０２１９】次に、上記解読したｒが乱数履歴に入っているか否かを認証手段７３の比較部７３ａは調べる。また上記解読したユーザ情報と第１の局１１から送信されてきたユーザ情報とを、比較部７３ｂを用いて比較する（図８の処理４１３）。解読した乱数ｒが乱数履歴に入っていた場合と、解読したI_aと受信したI_aが異なる場合との少なくとも一方が生じたら、認証手段７３は第１の局１１の正当性を認めない。

【０２２０】第１の局１１の正当性を認めないこととなった場合は、第２の局４１は認証動作を中止する。また第２の局４１は、通信を終了させたり、第１の局１１にエラーメッセージを出す等任意好適な処置をとる。

【０２２１】一方、解読した乱数ｒが乱数履歴になく、かつ、解読したユーザ情報と送信されてきたユーザ情報とが等しい場合、認証手段７３は、第１の局１１の正当性を認める。第１の局１１を正当と認めた場合（図８の処理４１４）、第２の局４１は、通信許可信号”ＯＫ”と共有暗号鍵生成のための関数g_jの番号ｊとを、第１の局１１に送信する（図８の通信４０２）。また、第２の局４１の共有鍵生成手段５３は、共有暗号鍵を

$K_{12}=g_j\ (r)$

のように生成する（図８の処理４１５）。

【０２２２】一方、通信許可信号”ＯＫ”を受信した第１の局１１は、共有鍵生成手段２３を用い共有暗号鍵を

$K_{12}=g_j(r)$
のように生成する（図８の処理４１６）。

【０２２３】この第４の実施の形態によれば、ユーザ情報と第三者に知られていない秘密情報とを用いて、第２の局が第１の局の正当性を認証することができる。しかも、認証の際に用いた情報である乱数をそのまま用いて第１の局および第２の局の間に暗号鍵の共有を実現している。しかも、第１の局の認証処理と、第１の局および第２の局の間の共有暗号鍵の生成処理とを連続的に行なうことができる。

【０２２４】またユーザ認証を行うとき、復号した乱数を乱数履歴と比較している。乱数は通信ごとに異なる。第３者が通信情報を盗聴してこれを用いて第２の局を繰り返して攻撃しようとしてもこの通信情報から復号される乱数は乱数履歴に存在する。すると第２の局はこの通信情報を正当と認めない。そのため第３者の繰り返し攻撃を防止することができる。

【０２２５】５．第５の実施の形態
次に、認証方法の第５の発明、暗号鍵共有方法の第３の発明、通信システムの第５および第１３の発明それぞれの実施の形態を、併せて説明する。

【０２２６】５－１．通信システムの構成説明
図９は第５の実施の形態の通信システムの構成を説明する図である。

【０２２７】この第５の実施の形態の通信システムは第４の実施の形態（図７）の通信システムを以下のように変更したものである。　：第１の局１１に、乱数生成手段２９の代わりに第１の乱数r_1および第２の乱数r_2を生成する乱数生成手段１２１を設ける。　：第１の局１１に、認証情報生成手段３３を設ける代わりに、第１の暗号文を生成する暗号文生成手段１２３と、暗号鍵生成手段１２５と、暗号鍵を用いて第１の暗号文をさらに暗号化して認証情報を生成する認証情報生成手段１２７とを設ける。　：第２の局４１に、認証情報復号手段６９と認証手段７３とを設ける代わりに、復号鍵生成手段７５と、復号鍵を用い認証情報を復号する認証情報復号手段７７と、復号されたユーザ情報に基づいて第１の局を認証する認証手段７９と、第１の乱数r_1を認証する乱数認証手段８１を設ける。

【０２２８】ここで、乱数生成手段１２１は、発生した乱数のうちの第２の乱数r_2を共有鍵生成手段２３と、暗号文生成手段１２３と、認証情報生成手段１２７とに出力できるように、これら構成成分２３、１２３、１２７と接続してある。さらに、第１の乱数r_1を暗号鍵生成手段１２５と送受信インタフェース１７とに出力できるよう、これら構成成分１２５、１７と接続してある。

【０２２９】暗号文生成手段１２３は、乱数生成手段１２１と、ユーザ情報格納部１５と、アルゴリズムＥテーブル３５と、認証情報生成手段１２７とに接続してある。この暗号文生成手段１２３は、乱数r_2を鍵としてユーザ情報I_aを暗号化して第１の暗号文を生成し、これを認証情報生成手段１２７に出力する手段である（詳細は後述する）。暗号化のための暗号化アルゴリズムは、ここではアルゴリズムＥテーブル３５より入力される。

【０２３０】暗号鍵生成手段１２５は、乱数生成手段１２１と、秘密情報格納部１３と、関数ｆテーブル１９と、認証情報生成手段１２７とに接続してある。この暗号鍵生成手段１２５は、認証情報を生成するための鍵を、第１の乱数r_1と秘密情報K_aと所定のアルゴリズムとにより生成し、これを認証情報生成手段１２７に出力する手段である（詳細は後述する）。ここでは、所定のアルゴリズムとして一方向性関数f_iを用いる。一方向性関数f_iは、関数ｆテーブル１９より入力される。

【０２３１】認証情報生成手段１２７は、暗号鍵生成手段１２５で生成される暗号鍵を用いて、第２の乱数r_2と前記第１の暗号文とを暗号化して認証情報を生成する手段である（詳細は後述する）。この暗号化の際の暗号化アルゴリズムはアルゴリズムＥテーブル３５より入力される。認証情報生成手段１２７の出力は送受信インターフェース１７に接続してある。

【０２３２】第２の局４１の復号鍵生成手段７５は、送信されてくる第１の乱数r_1と秘密情報K'_aと所定のアルゴリズムとにより、認証情報を復号するための鍵（復号鍵）を生成する手段である（詳細は後述する。）。ここでは、所定のアルゴリズムとして一方向性関数f_iを用いる。一方向性関数f_iは、関数ｆテーブル４７より入力される。復号鍵生成手段７５の出力は認証情報復号手段７７に接続してある。

【０２３３】認証情報復号手段７７は、復号鍵生成手段７５で生成された復号鍵を用いて認証情報を復号する手段である（詳細は後述する）。復号化のためのアルゴリズムは、ここではアルゴリズムＥテーブル７１より入力される。認証情報復号手段７７の出力は認証手段７９に接続してある。

【０２３４】認証手段７９は、この場合、復号されたユーザ情報と送信されてきたユーザ情報とを比較することにより、第１の局１１の正当性を認証する手段である（詳細は後述する）。

【０２３５】第１の乱数を認証する手段８１は、今回送信されてきた第１の乱数r_1が過去に送信されてきた乱数の履歴中に含まれるか否かを調べて、第１の局の正当性を認証する手段である（詳細は後述する）。

【０２３６】上記説明した手段以外は、第４の実施の形態と同じとしてある。

【０２３７】５－２．動作の説明
次に、第５の実施の形態の通信システムの動作を説明する。これにより、認証方法および共有暗号鍵の生成方法の処理手順を説明する。この説明を図９に加えて図１０を参照して行なう。図１０は処理の流れを示した図であ

る。

【０２３８】第１の局１１の乱数生成手段１２１は通信のごとに第１の乱数r_1およびr_2を生成する。第１の局１１の暗号文生成手段１２３は、第２の乱数r_2を鍵として、かつ、暗号アルゴリズムE_qを使って、ユーザ情報I_aを暗号化し、第１の暗号文ここではE_q｛r_2，I_a｝という暗号文を生成する。また第１の局１１の暗号鍵生成手段１２５は、認証情報を生成するための暗号アルゴリズムの鍵としてここではf_i（r_1，K_a）を生成する。そして、認証情報生成手段１２７は、暗号鍵f_i（r_1，K_a）を用いて、かつ、暗号アルゴリズムE_qを使って、乱数r_2と第１の暗号文E_q｛r_2，I_a｝をさらに暗号化し、認証情報としてのE_q｛f_i（r_1，K_a），（r_2｜E_q｛r_2，I_a｝）｝を生成する（図１０の処理５１１）。

【０２３９】次に、第１の局１１は、ユーザ情報I_a、第１の乱数r_1、一方向性関数番号i、暗号化アルゴリズム番号qおよび認証情報E_q｛f_i（r_1，K_a），（r_2｜E_q｛r_2，I_a｝）｝を、第２の局４１に送信する（図１０の通信５０１）。

【０２４０】次に、第２の局４１は、ユーザ情報I_aを用いて、第１の局１１についての乱数履歴と秘密情報K'_aとを、ユーザ情報・乱数履歴情報・秘密情報格納部６３から見つけ出す。次にまず、第２の局４１の乱数認証手段８１が、乱数履歴を調べて（図１０の処理５１２）、もし受信した第１の乱数r_1が乱数履歴に入っているならば第１の局１１の正当性を認めない。

【０２４１】乱数履歴を調べた結果、第１の局１１の正当性を認めないこととなった場合は、第２の局４１は認証動作を中止する。そして第２の局４１は、通信を終了させたり、第１の局１１にエラーメッセージを出す等任意好適な処置をとる。

【０２４２】一方、今回送信されてきた第１の乱数r_1が乱数履歴に含まれていなかった場合は、第２の局４１の復号鍵生成手段７５が復号鍵としてf_i（r_1，K'_a）を生成する。次に、第２の局４１の認証情報復号手段７７が、上記復号鍵f_i（r_1，K'_a）を用いて、認証情報E_q｛f_i（r_1，K_a），（r_2｜E_q｛r_2，I_a｝）｝を復号すなわち解読して第２の乱数r_2を得る。さらに第２の局４１の認証情報復号手段７７が、上記解読した第２の乱数r_2を鍵として用い、第１の暗号文E_q｛r_2，I_a｝を復号すなわち解読してユーザ情報I_aを得る（図１０の処理５１３）。

【０２４３】また、第２の局４１は今回送信されてきた第１の乱数r_1を、ユーザ情報・乱数履歴情報・秘密情報格納部６３に、乱数履歴情報として追加する。

【０２４４】次に、第２の局４１の認証手段７９は、復号したユーザ情報と送信されてきたユーザ情報とを比較する（図１０の処理５１４）。この比較において両者が等しければ（図１０の処理５１５）、第２の局４１は、第１の局１１の正当性を認め、通信許可信号”ＯＫ”と共有暗号鍵生成のための関数g_jの番号jとを、第１の局１１に送信する（図１０の通信２０２）。また、第２の局４１の共有鍵生成手段５３は、共有暗号鍵を

$K_{12}=g_j$（r_2）

のように生成する（図１０の処理５１６）。

【０２４５】一方、通信許可信号”ＯＫ”を受信した第１の局１１は、共有鍵生成手段２３を用い共有暗号鍵を

$K_{12}=g_j$（r_2）

のように生成する（図１０の処理５１７）。

【０２４６】この第５の実施の形態によれば、ユーザ情報と第三者に知られていない秘密情報とを用いて、第２の局が第１の局の正当性を認証することができる。しかも、認証の際に用いた情報である第２の乱数r_2をそのまま用いて第１の局および第２の局の間に暗号鍵の共有を実現している。しかも、第１の局の認証処理と、第１の局および第２の局の間の共有暗号鍵の生成処理とを連続的に行なうことができる。

【０２４７】また送信されてきた第１の乱数r_1が乱数履歴に含まれるか否かで、第１の局の正当性を判断することができる。そのため、正当でない通信者による繰り返し攻撃を防止することができる。

【０２４８】また、秘密情報をそのまま暗号鍵にしないで所定のアルゴリズムを用いて秘密情報を暗号鍵化するので、第４の実施の形態に比べ秘密保護能力が高いといえる。

【０２４９】また、２種類の乱数r_1，r_2を用いているのでその分、秘密保護能力が高いといえる。

【０２５０】６．第６の実施の形態

次に、認証方法の第６の発明、暗号鍵共有方法の第２の発明、通信システムの第６および第１２の発明それぞれの実施の形態を、併せて説明する。

【０２５１】６－１．通信システムの構成説明

図１１は第６の実施の形態の通信システムの構成を説明する図である。

【０２５２】この第６の実施の形態の第４の実施の形態（図７）との主な相違点は、　：第１の局１１に、第３の実施の形態と同じくアクセス回数計数手段３１を設けた点と、　：第１の局１１に、認証情報生成手段３３を設ける代わりに、ユーザ情報とアクセス回数とを暗号化する暗号化手段１２９と、暗号化手段１２９で暗号化された暗号をさらに暗号化し認証情報を生成する認証情報生成手段１３１とを設けた点と、　：第２の局４１に、認証手段７３の代わりに、復号されたユーザ情報およびアクセス回数に基づいて第１の局の正当性を認証する認証手段８３を設けた点と、　：第２の局４１に、ユーザ情報・乱数履歴情報・秘密情報格納部６３の代わりに、第３の実施の形態と同じく、ユーザ情報・アクセス回数・秘密情報格納部６７（ただし、この場合は復号されたアクセス回数を記憶する）を設けた点である。

【０２５３】ここで、暗号化手段１２９は、乱数ｒを鍵としてユーザ情報Ｉａとアクセス回数ｎａとを暗号化する手段である（詳細は後述する）。暗号化のための暗号化アルゴリズムは、ここではアルゴリズムＥテーブル３５より入力される。この暗号化手段１２９の出力は、認証情報生成手段１３１に接続してある。

【０２５４】認証情報生成手段１３１は、乱数と暗号化手段１２９で暗号化されたユーザ情報Ｉａとアクセス回数ｎａとを、秘密情報Ｋａを鍵としてさらに暗号化して認証情報を生成する手段である（詳細は後述する）。この暗号化の際の暗号化アルゴリズムはアルゴリズムＥテーブル３５より入力される。認証情報生成手段１３１の出力は送受信インタフェース１７に接続してある。

【０２５５】第２の局４１の認証手段８３は、認証情報復号手段６９で復号されたユーザ情報と第１の局から送信されてくるユーザ情報とを比較する比較部８３ａと、認証情報復号手段６９で復号されたアクセス回数ｎａと格納部６７に記憶してあるアクセス回数ｎ'ａとの間に所定の不等式関係が成立するか否かを比較する比較部８３ｂとで構成してある。所定の不等式とは例えばｎ'ａ＋ε＞ｎａ＞ｎ'ａとすることができる。ここでεは通信ミスなどを許容する数で例えば５程度である。この認証手段８３は、２つの比較部８３ａ、８３ｂでそれぞれ比較結果が合格となった場合に、第１の局を正当と認証する。

【０２５６】上記以外の構成は第４の実施の形態と同じとしてある。

【０２５７】６－２．動作の説明

次に、第６の実施の形態の通信システムの動作を説明する。これにより、認証方法および共有暗号鍵の生成方法の処理手順を説明する。この説明を図１１に加えて図１２を参照して行なう。図１２は処理の流れを示した図である。

【０２５８】第１の局１１の乱数生成手段２９は、通信の際乱数ｒを生成する。第１の局１１のアクセス回数計数手段３１は、計数値すなわちアクセス回数ｎａを１増加させ、ｎａ＝ｎａ＋１とする。第１の局の暗号化手段１２９は、乱数ｒを鍵としてかつ暗号アルゴリズムＥｑを使って、ユーザ情報Ｉａとアクセス回数ｎａとを暗号化しここではＥｑ｛ｒ，Ｉａ｜ｎａ｝という暗号文を生成する。そして第１の局１１の認証情報生成手段１３１は、秘密情報Ｋａを鍵として、かつ、暗号アルゴリズムＥｑを使って、乱数と上記の暗号文Ｅｑ｛ｒ，Ｉａ｜ｎａ｝をさらに暗号化し、認証情報としてのＥｑ｛Ｋａ，（ｒ｜Ｅｑ｛ｒ，Ｉａ｜ｎａ｝）｝を生成する（図１２の処理６１１）。

【０２５９】次に、第１の局１１は、ユーザ情報Ｉａ、暗号化アルゴリズム番号ｑおよび認証情報Ｅｑ｛Ｋａ，（ｒ｜Ｅｑ｛ｒ，Ｉａ｜ｎａ｝）｝を、第２の局４１に送信する（図１２の通信６０１）。

【０２６０】次に、第２の局４１は、ユーザ情報Ｉａを用いて、第１の局１１についての秘密情報Ｋ'ａと、いままでのアクセス回数ｎａ'とを、ユーザ情報・アクセス回数・秘密情報格納部６３から見つけ出す。

【０２６１】次に第２の局４１は認証情報復号化手段６９を用いて、秘密情報Ｋ'ａを鍵として、認証情報である暗号文Ｅｑ｛Ｋａ，（ｒ｜Ｅｑ｛ｒ，Ｉａ｜ｎａ｝）｝を復号してすなわち解読して、乱数ｒを得る。さらに、ｒを鍵にＥｑ｛ｒ，Ｉａ｜ｎａ｝を復号してすなわち解読して、Ｉａとｎａとを得る（図１２の処理６１２）。

【０２６２】次に、上記解読したユーザ情報と第１の局１１から送信されてきたユーザ情報とを、認証手段８３の比較部８３ａ用いて比較する。さらに、上記解読したアクセス回数ｎａがｎ'ａ＋ε＞ｎａ＞ｎ'ａを満たすか否かを、比較部８３ｂを用いて調べる（図１２の処理６１３）。解読したアクセス回数ｎａが上記不等式を満たしていない場合と、解読したＩａと受信したＩａとが等しくない場合の少なくとも一方が生じたら、認証手段８３は第１の局１１の正当性を認めない。

【０２６３】第１の局１１の正当性を認めないこととなった場合は、第２の局４１は認証動作を中止する。また第２の局４１は、通信を終了させたり、第１の局１１にエラーメッセージを出す等任意好適な処置をとる。

【０２６４】一方、解読したアクセス回数ｎａが上記不等式を満たし、かつ、解読したユーザ情報と送信されてきたユーザ情報とが等しい場合、認証手段８３は、第１の局１１の正当性を認める。第１の局１１を正当と認めた場合（図１２の処理６１４）、第２の局４１は、通信許可信号”ＯＫ”と共有暗号鍵生成のための関数ｇｊの番号ｊとを、第１の局１１に送信する（図１２の通信６０２）。しかも、格納部６７に記憶してあるアクセス回数ｎ'ａをｎａに変更する（図１２の処理６１５）。また、第２の局４１の共有鍵生成手段５３は、共有暗号鍵を

$K_{12}=g_j\ (r)$

のように生成する（図１２の処理６１６）。

【０２６５】一方、通信許可信号”ＯＫ”を受信した第１の局１１は、共有鍵生成手段２３を用い共有暗号鍵を

$K_{12}=g_j\ (r)$

のように生成する（図１２の処理６１７）。

【０２６６】この第６の実施の形態によれば、ユーザ情報と第三者に知られていない秘密情報とを用いて、第２の局が第１の局の正当性を認証することができる。しかも、認証の際に用いた情報である乱数ｒをそのまま用いて第１の局および第２の局の間に暗号鍵の共有を実現している。しかも、第１の局の認証処理と、第１の局および第２の局の間の共有暗号鍵の生成処理とを連続的に行なうことができる。

【０２６７】また第１の局の認証をおこなうとき、ユーザ情報とアクセス回数との両方を用い行なうので認証の信頼性を高めることができる。

【０２６８】さらにこの第６の実施の形態では通信ごとに値が変わるアクセス回数（認証情報から復号したアクセス回数）を認証している。もし通信情報を第３者が盗聴してそれを用いて第２の局を繰り返して攻撃した場合それはアクセス回数の部分がいつも同じ値の攻撃となるから、それは正当な通信とされない。そのため、第３者の繰り返し攻撃を防止することができる。

【０２６９】７．第７の実施の形態

次に、認証方法の第７の発明、暗号鍵共有方法の第３の発明、通信システムの第７および第１３の発明それぞれの実施の形態を、併せて説明する。

【０２７０】７－１．通信システムの構成説明

図１３は第７の実施の形態の通信システムの構成を説明する図である。

【０２７１】この第７の実施の形態の通信システムは、第５の実施の形態（図９）の通信システムを以下のように変更したシステムに相当する。　：第１の局１１に、第３の実施の形態と同じくアクセス回数計数手段３１を設ける。　：第５の実施の形態で用いていた暗号文生成手段１２３の代わりに、第２の乱数r_2を鍵としてユーザ情報I_aとアクセス回数n_aとを暗号化して第１の暗号文を生成する暗号文生成化手段１３３を設ける。　：第５の実施の形態で第２の局４１に設けていた乱数認証手段８１を省略する。　：第５の実施の形態で設けていた認証手段７９の代わりに、第６の実施の形態と同じく復号されたユーザ情報およびアクセス回数に基づいて第１の局を認証する認証手段８３を設ける。

【０２７２】それ以外の構成は第５の実施の形態と同じとしている。

【０２７３】７－２．動作の説明

次に、第７の実施の形態の通信システムの動作を説明する。これにより、認証方法および共有暗号鍵の生成方法の処理手順を説明する。この説明を図１３に加えて図１４を参照して行なう。図１４は処理の流れを示した図である。

【０２７４】第１の局１１の乱数生成手段１２１は通信のごとに第１の乱数r_1およびr_2を生成する。第１の局１１のアクセス回数計数手段３１は、計数値すなわちアクセス回数n_aを１増加させ、$n_a = n_a + 1$とする。第１の局１１の暗号文生成手段１３３は、第２の乱数r_2を鍵として、かつ、暗号化アルゴリズムE_qを使って、ユーザ情報I_aとアクセス回数n_aとを暗号化して第１の暗号文ここでは$E_q\{r_2, I_a | n_a\}$という暗号文を生成する。また第１の局１１の暗号鍵生成手段１２５は、認証情報を生成するための暗号アルゴリズムの鍵としてここでは$f_i(r_1, K_a)$を生成する。そして、認証情報生成手段１２７は、暗号鍵$f_i(r_1, K_a)$を用いて、かつ、暗号化アルゴリズムE_qを使って、乱数r_2と第１の暗号文$E_q\{r_2, I_a | n_a\}$をさらに暗号化し、認証情報としての$E_q\{f_i(r_1, K_a), (r_2 | E_q\{r_2, I_a | n_a\})\}$を生成する（図１４の処理７１１）。

【０２７５】次に、第１の局１１は、ユーザ情報I_a、第１の乱数r_1、一方向性関数番号i、暗号化アルゴリズム番号qおよび認証情報$E_q\{f_i(r_1, K_a), (r_2 | E_q\{r_2, I_a | n_a\})\}$を、第２の局４１に送信する（図１４の通信７０１）。

【０２７６】次に、第２の局４１は、ユーザ情報I_aを用いて、第１の局１１についての秘密情報K'_aといままでのアクセス回数n_a'とを、ユーザ情報・アクセス回数・秘密情報格納部６７から見つけ出す。

【０２７７】次に第２の局４１は認証情報復号化手段６９を用いて、$f_i(r_1, K'_a)$を鍵として、認証情報である暗号文$E_q\{f_i(r_1, K_a), (r_2 | E_q\{r_2, I_a | n_a\})\}$を復号してすなわち解読して、第２の乱数$r_2$を得る。さらに、第２の乱数$r_2$を鍵に$E_q\{r_2, I_a | n_a\}$を復号してすなわち解読して、$I_a$と$n_a$とを得る（図１４の処理７１２）。

【０２７８】次に、上記解読したユーザ情報と第１の局１１から送信されてきたユーザ情報とを、認証手段８３の比較部８３ａ用いて比較する。さらに、上記解読したアクセス回数n_aが$n'_a + \varepsilon > n_a > n'_a$を満たすか否かを、比較部８３ｂを用いて調べる（図１４の処理７１３）。解読したアクセス回数n_aが上記不等式を満たしていない場合と、解読したI_aと受信したI_aとが等しくない場合の少なくとも一方が生じたら、認証手段８３は第１の局１１の正当性を認めない。

【０２７９】第１の局１１の正当性を認めないこととなった場合は、第２の局４１は認証動作を中止する。また第２の局４１は、通信を終了させたり、第１の局１１にエラーメッセージを出す等任意好適な処置をとる。

【０２８０】一方、解読したアクセス回数n_aが上記不等式を満たし、かつ、解読したユーザ情報と送信されてきたユーザ情報とが等しい場合、認証手段８３は、第１の局１１の正当性を認める。第１の局１１を正当と認めた場合（図１４の処理７１４）、第２の局４１は、通信許可信号”ＯＫ”と共有暗号鍵生成のための関数g_iの番号jとを、第１の局１１に送信する（図１４の通信７０２）。しかも、格納部６７に記憶してあるアクセス回数n'_aをn_aに変更する（図１４の処理７１５）。また、第２の局４１の共有鍵生成手段５３は、共有暗号鍵を

$K_{12} = g_j(r_2)$

のように生成する（図１４の処理７１６）。

【０２８１】一方、通信許可信号”ＯＫ”を受信した第１の局１１は、共有鍵生成手段２３を用い共有暗号鍵を

$K_{12} = g_j(r_2)$

のように生成する（図１４の処理７１７）。

【０２８２】この第７の実施の形態によれば、ユーザ情報と第三者に知られていない秘密情報とを用いて、第２

の局が第１の局の正当性を認証することができる。しかも、認証の際に用いた情報である第２の乱数ｒ２をそのまま用いて第１の局および第２の局の間に暗号鍵の共有を実現している。しかも、第１の局の認証処理と、第１の局および第２の局の間の共有暗号鍵の生成処理とを連続的に行なうことができる

【０２８３】また第１の局の認証をおこなうとき、ユーザ情報とアクセス回数との両方を用い行なうので認証の信頼性を高めることができる。

【０２８４】また、認証情報を生成するとき、乱数ｒ２を鍵として第１の暗号化をし、一方向性関数の値を鍵として第２の暗号化をしているので、第６の実施の形態に比べ機密保護性能が高まる。

【０２８５】さらにこの第７の実施の形態では通信ごとに値が変わるアクセス回数（認証情報から復号したアクセス回数）を認証している。もし通信情報を第３者が盗聴してそれを用いて第２の局を繰り返して攻撃した場合それはアクセス回数の部分がいつも同じ値の攻撃となるから、それは正当な通信とされない。そのため、第３者の繰り返し攻撃を防止することができる。

【０２８６】８．第８の実施の形態

次に、認証方法の第８の発明、暗号鍵共有方法の第４の発明、通信システムの第８および第１４の発明それぞれの実施の形態を、併せて説明する。図１５は、この第８の実施の形態の通信システムの構成を説明する図である。

【０２８７】この第８の実施の形態は、通信を希望する第１の局１１および第２の局４１と、第２の局に代わって認証をする信頼できる第３の局１５１とを含む通信システムにおいて、第１の局１１の正当性を第２の局に代わって第３の局が認証しながら第１の局および第２の局の間に暗号鍵を共有するケースである。ただし前提条件として、第１の局１１と第３の局１５１とが秘密情報を共有している。しかも、第２の局４１と第３の局１５１との間の通信経路は安全であると仮定する。

【０２８８】この第８の実施の形態は、例えば、第１の局１１が外界の多数の個人端末であり、第３の局１５１が企業内の多数の端末であり、第２の局４１が第３の局のファイアウォールであるような通信システムに適用できる。そして、第２の局４１の負荷を分散でき、また通信システムの秘密保護能力をより高めることが可能になる例である。以下、詳細に説明する。

【０２８９】８－１．通信システムの構成説明

第１の局１１は、秘密情報K_aを格納する秘密情報格納部１３と、ユーザ情報I_aを格納するユーザ情報格納部１５と、他局との送受信のための送受信インターフェース１７と、乱数生成手段１４１と、認証情報生成手段１４３と、共有鍵生成手段２３と、共有鍵格納部２７とを具える。これら構成成分の接続関係は、第２の実施の形態（図３参照）での接続関係と同じ（関数ｆテーブル、関数ｇテーブルを除いて同じ）としてある。

【０２９０】第２の局４１は、他局との送受信のための送受信インターフェース４５と、これに接続された共有鍵格納部９１とを具える。なお第１の局１１および第２の局４１の間は、通信回線１００ａにより接続してある。

【０２９１】第３の局１５１は、正当な通信者ごとの少なくともユーザ情報I_aおよび秘密情報K'_aを格納するユーザ情報・秘密情報格納部１５３と、送受信インターフェース１５５と、認証手段１５７と、共有鍵生成手段１５９とを具える。第２の局４１および第３の局１５１の間は、通信回線１００ｂにより接続してある。

【０２９２】ユーザ情報・秘密情報格納部１５３は、送受信インタフェース１５５と、認証手段１５７と、共有鍵生成手段１５９とに接続してある。認証手段１５７は送受信インタファース１５５に接続してある。共有鍵生成手段１５９は送受信インタファース１５５に接続してある。

【０２９３】なお、ユーザ情報・秘密情報格納部１５３について少なくともユーザ情報I_aおよび秘密情報K'_aを格納すると述べたのは、認証方法次第では、乱数履歴、アクセス回数、復号した乱数履歴または復号したアクセス回数を記憶する場合があっても良いという意味である。また、秘密情報K_a、K'_aは同じものであるが、第１、第３のどちらの局側の秘密情報かを区別するために、K_a、K'_aと称している。

【０２９４】ここで、第１の局１１の認証情報生成手段１４３は、乱数生成手段１４１で発生される乱数と秘密情報格納部１３に格納してある秘密情報K_aとを用い認証情報を生成するものであれば、任意好適なものとできる。例えば、一方向性関数f_iを用いたり、または、暗号化アルゴリズムを用いて認証情報を生成することができる。具体的には、　：第１の実施の形態で説明した手段２１、　：第４の実施の形態で説明した手段３３、　：第５の実施の形態で説明した手段１２３、１２５および１２７を含む手段、　：第６の実施の形態で説明した手段１２９および１３１を含む手段、または、　：第７の実施の形態で説明した手段１２５、１２７および１３３を含む手段、により認証情報生成手段を構成することができる。もちろん、認証情報生成手段１４３を上記の　～　のいずれかで構成する場合は、それについて説明した第１～第７の実施の形態のいずれかの教示に従い、第１の局内の構成を変更する。

【０２９５】また乱数生成手段１４１は例えば通信ごとに乱数ｒを発生する手段である。この乱数生成手段１４１は、認証情報生成手段１４３と、共有鍵生成手段２３と、送受信インタフェース１７とに接続してある。なお、乱数生成手段１４１は、認証情報生成手段１４３の構成の仕方によっては、第１の乱数r_1および第２の乱数r_2を生成する手段としても良い。

【０２９６】また第３の局１５１の認証手段１５７は、第１の局１１からの認証情報を秘密情報K'aを用い認証する手段である。この認証手段１５７の構成は、第１の局１１の認証情報生成手段１４３をどのように構成したかに応じ決める。認証情報生成手段１４３を上記の　～　のいずれかで構成する場合は、それに対応して、(1) 第１の実施の形態で説明した手段５１および５９を含む手段、(2) 第４の実施の形態で説明した手段６９および７３を含む手段、(3) 第５の実施の形態で説明した手段７５、７７および７９を含む手段、(4) 第６の実施の形態で説明した手段６９および８３を含む手段、または、(5) 第７の実施の形態で説明した手段７５、７７および８３を含む手段、により認証手段１５７を構成することができる。もちろん、認証手段１４３を上記の(1) ～(5) のいずれかで構成する場合は、それについて説明した第１～第７の実施の形態のいずれかの教示に従い第３の局内の構成を変更する。

【０２９７】また、第１の局１１の共有鍵生成手段２３および共有鍵格納部２７は、それぞれ、第１～第７の実施の形態にて説明した手段２３、２７で構成できる。第３の局１５１の共有鍵生成手段１５９は、認証手段１５７が第１の局を正当と判断したときに、認証に用いた情報のうちの１または複数を用い、共有暗号鍵を生成する手段である。また、第２の局４１の共有鍵格納部９１は、第３の局で生成されそこから送信されてくる共有鍵を格納する手段である。

【０２９８】８－２．動作の説明

次に、第８の実施の形態の通信システムの動作を説明する。これにより、認証方法および共有暗号鍵の生成方法の処理手順を説明する。この説明を図１５に加えて図１６を参照して行なう。図１６は処理の流れを示した図である。

【０２９９】第１の局１１の乱数生成手段１４１は通信に当たり乱数ｒを発生する。第１の局の認証情報生成手段１４３は乱数ｒと秘密情報K_aとを用いて認証情報A_aを生成する（図１６の処理８１１）。この認証情報A_aは、すでに説明したように、認証情報生成手段１４３の構成次第で任意のものとなる。

【０３００】次に、第１の局１１は、乱数ｒとユーザ情報I_aと認証情報A_aとを、第２の局４１に送信する（図１６の通信８０１）。

【０３０１】第２の局４１は、秘密情報と認証機能をもっていないので、第１の局１１から送られた乱数ｒとユーザ情報I_aと認証情報A_aとを第３の局１５１に転送する（図１６の通信８０２）。

【０３０２】第３の局１５１は、第２の局４１から転送されきたユーザ情報I_aを用いユーザ情報・秘密情報格納部１５３から第１の局１１についての秘密情報K'aを見つけ出す。そして、第２の局４１から転送されきた認証情報A_aを、第３の局１５１は秘密情報K'aを用いて認証する（図１６の処理８１３）。この認証は例えば次のように行うことができる。認証情報A_aは、乱数ｒと秘密情報K_aとを用いたものであるので、第３の局１５１は認証情報A_aから秘密情報K'aを用い乱数ｒを得ることができる。また、別途に乱数ｒは送信されている。したがって、認証情報から得た乱数と送信されてきた乱数とを比較することで、第１の局の正当性を認証することができる。もちろん、秘密情報K'aを用いて認証する具体的な方法は、すでに説明したが、認証情報生成１４３や認証手段１５７それぞれをどのように構成するかで変更することができる。

【０３０３】上記の認証において第１の局が正当とされた場合（図１６の処理８１４）、第３の局１５１の共有鍵生成手段１５９は共有暗号鍵K_{12}を生成する（図１６の処理８１５）。また、第３の局１５１は、生成した共有暗号鍵K_{12}と、通信許可信号”ＯＫ”とを第２の局４１に送信する（図１６通信８０３）。なお共有暗号鍵K_{12}の生成アルゴリズムは、第１および第３の局の間で決めた任意のアルゴリズムとできる。例えば乱数および秘密情報K_aを使ってg_j（ｒ，K_a）のように作成することができる。もちろん、関数ｇテーブルを用いるような方法でも良い。

【０３０４】共有暗号鍵K_{12}と通信許可信号”ＯＫ”とを受信した第２の局４１は、共有暗号鍵K_{12}を共有鍵格納部９１に格納し、また、通信許可信号”ＯＫ”を第１の局１１に送信する（図１６の通信８０４）。

【０３０５】通信許可信号”ＯＫ”を受信した。第１の局１１は共有暗号鍵K_{12}を生成し（図１６の処理８１６）、これを共有鍵格納部２７に格納する。

【０３０６】この第８の実施の形態によれば、秘密情報を共有しかつ認証情報と共有鍵の生成手段とを持つ第１の局および第３の局の間に、秘密情報を持たない第２の局が介在しても、第１の局の認証を実現することができ、然も第１の局および第２の局の間での暗号鍵の共有を実現することができる。また信頼できる第３の局が第２の局に代わって第１の局の正当性を認証するので、第２の局の負荷を減らすことができる。特に、第１の局と第３の局それぞれが多数の端末からなるグループの場合、第２の局の負荷分散が実現される。

【０３０７】またこの第８の実施の形態の場合も、認証の際に用いた情報を用いて第１の局および第２の局の間に暗号鍵の共有を実現している。しかも、第１の局の認証処理と、第１の局および第２の局の間の共有暗号鍵の生成処理とを連続的に行なうことができる。

【０３０８】９．第９の実施の形態

次に、認証方法の第９の発明、暗号鍵共有方法の第４の発明、通信システムの第９および第１４の発明それぞれの実施の形態を、併せて説明する。

【０３０９】図１７は第９の実施の形態の通信システムの構成を説明する図である。第８の実施の形態では乱数

生成手段を第1の局11内に設ける例を説明した。これに対し、この第9の実施の形態では、第2の局41に乱数生成手段93を設けた例である。それ以外の構成は第8の実施の形態と同様としてある。

【0310】第2の局41に設けた乱数生成手段93は、送受信インタフェース45に接続している。しかも、乱数生成手段93が発生した乱数は、第1の局11の認証情報生成手段143および共有鍵生成手段23と、第3の局151の認証手段157および共有鍵生成手段159に送信される構成としてある。なお、認証情報生成手段143および認証手段157の構成が、第5の実施の形態などのように乱数r_1および乱数r_2を用いる場合は、乱数生成手段93も乱数r_1および乱数r_2を発生する構成とする。

【0311】次に、第9の実施の形態の通信システムの動作について、図17に加えて図18を参照して説明する。図18は処理の流れを示した図である。

【0312】第1の局11は第2の局41にユーザ情報I_aを送信する（図18の通信901）。

【0313】第2の局41はユーザ情報I_aを受信すると乱数生成手段93を用いて乱数rを発生しこれを第1の局11に返信する（図18の通信902）。

【0314】第1の局11の認証情報生成手段143は、乱数rと秘密情報K_aとを用い認証情報A_aを生成し（図18の処理911）、これを第2の局41に送信する（図18の通信903）認証情報A_aを受信した第2の局41は、認証情報A_aと乱数rとユーザ情報I_aとを、第3の局151に送信する（図18の通信904）。

【0315】第3の局151は、第2の局41から送信されきたユーザ情報I_aを用いユーザ情報・秘密情報格納部153から第1の局11についての秘密情報K'_aを見つけ出す。そして、第2の局41から転送されきた認証情報A_aを、第3の局151は秘密情報K'_aを用いて認証する（図18の処理912）。この認証は例えば第8の実施の形態で説明したように行うことができる。

【0316】上記の認証において第1の局が正当とされた場合（図18の処理913）、第3の局151の共有鍵生成手段159は共有暗号鍵K_{12}を生成する（図18の処理914）。また、第3の局151は、生成した共有暗号鍵K_{12}と、通信許可信号”OK”とを第2の局41に送信する（図18通信905）。

【0317】共有暗号鍵K_{12}と通信許可信号”OK”とを受信した第2の局41は、共有暗号鍵K_{12}を共有鍵格納部91に格納し、また、通信許可信号”OK”を第1の局11に送信する（図18の通信906）。

【0318】通信許可信号”OK”を受信した第1の局11は、共有暗号鍵生成手段23を用い共有暗号鍵K_{12}を生成し（図18の処理915）、これを共有鍵格納部27に格納する。

【0319】この第9の実施の形態によれば、秘密情報を共有しかつ認証情報と共有鍵の生成手段とを持つ第1の局および第3の局の間に、秘密情報を持たない第2の局が介在しても、第1の局の認証を実現することができ、然も第1の局および第2の局の間での暗号鍵の共有を実現することができる。また信頼できる第3の局が第2の局に代わって第1の局の正当性を認証するので、第2の局の負荷を減らすことができる。特に、第1の局と第3の局それぞれが多数の端末からなるグループの場合、第2の局の負荷分散が実現される。

【0320】またこの第9の実施の形態の場合も、認証の際に用いた情報を用いて第1の局および第2の局の間に暗号鍵の共有を実現している。しかも、第1の局の認証処理と、第1の局および第2の局の間の共有暗号鍵の生成処理とを連続的に行なうことができる。

【0321】またこの第9の実施の形態の場合は乱数を第2の局が発生するので、第1の局自体が自ら適正な乱数を得ることができない。そのためもし第3者が第2の局に繰り返し攻撃を行おうとしても、それを防止することができる。

【0322】10．第10の実施の形態

次に、認証方法の第10の発明、暗号鍵共有方法の第5の発明、通信システムの第10および第15の発明それぞれの実施の形態を、併せて説明する。

【0323】図19は、この第10の実施の形態の通信システムの構成を説明する図である。

【0324】この第10の実施の形態は、通信を希望する第1の局11および第2の局41と、これら局11、41間に介在する中間局161とを含む通信システムにおいて、第1の局11の正当性を第2の局が認証しながら第1の局および第2の局の間で暗号鍵を共有するケースである。ただし前提条件として、第1の局11と第3の局151とが秘密情報を共有している。しかも、中間局161が乱数生成手段を具えている。しかも、中間局161と第1の局11との間の通信経路、中間局161と第2の局41との間の通信経路が安全か否かは問わない。

【0325】10－1．通信システムの構成説明

第1の局11は、乱数生成手段を省略した点を除いて第8の実施の形態の場合の第1の局と同じ構成としてある。

【0326】第2の局41は、他局との送受信のための送受信インターフェース45と、正当な通信者ごとの少なくともユーザ情報I_aおよび秘密情報K'_aを格納するユーザ情報・秘密情報格納部95と、認証手段97と、共有鍵生成手段99と、共有鍵格納部57とを具える。ユーザ情報・秘密情報格納部95は、送受信インタフェース45と、認証手段97と、共有鍵生成手段99とに接続してある。認証手段97は送受信インタフェース45に接続してある。共有鍵生成手段99は送受信インタ

フェース４５に接続してある。

【０３２７】なお、ユーザ情報・秘密情報格納部９５について少なくともユーザ情報I_aおよび秘密情報K'_aを格納すると述べたのは、認証方法次第では、乱数履歴、アクセス回数、復号した乱数履歴または複合したアクセス回数を記憶する場合があっても良いという意味である。

【０３２８】認証手段９７は、第１の局１１から中間局１６１を介し送信されてくる認証情報A_aを、格納部９５に格納してある秘密情報K'_aを用い認証する手段である。この認証手段９７は、第１の局１１の認証情報生成手段１４３の構成に応じた構成とする。

【０３２９】中間局１６１は、他局との送受信のための送受信インターフェース１６３と、これに接続された乱数生成手段１６５とを具える。乱数生成手段１６５が発生した乱数は、第１の局１１の認証情報生成手段１４３および共有鍵生成手段２３と、第２の局４１の認証手段９７および共有鍵生成手段９９に送信できる構成としてある。

【０３３０】第１の局１１と中間局１６１とは通信回線１０１ｃにより接続してあり、第２の局４１と中間局１６１とは通信回線１０１ｄにより接続してある。

【０３３１】１０－２．動作の説明

次に、第１０の実施の形態の通信システムの動作について、図１９に加えて図２０を参照して説明する。図２０は処理の流れを示した図である。

【０３３２】第１の局１１は中間局１６１にユーザ情報I_aを送信する（図２０の通信１００１）。

【０３３３】中間局１６１はユーザ情報I_aを受信すると乱数生成手段１６５を用いて乱数ｒを発生しこれを第１の局１１に返信する（図２０の通信１００２）。

【０３３４】第１の局１１の認証情報生成手段１４３は、乱数ｒと秘密情報K_aとを用い認証情報A_aを生成し（図２０の処理９１１）、これを中間局１６１に送信する（図２０の通信１００３）

認証情報A_aを受信した中間局１６１、認証情報A_aと乱数ｒとユーザ情報I_aとを、第２の局４１に送信する（図２０の通信１００４）。

【０３３５】第２の局４１は、中間局１６１から送信されきたユーザ情報I_aを用いユーザ情報・秘密情報格納部９５から第１の局１１についての秘密情報K'_aを見つけ出す。そして、中間局１６１から転送されきた認証情報A_aを、第２の局４１は、秘密情報K'_aを用いて認証する（図２０の処理１０１２）。この認証は例えば第８の実施の形態で説明したように行うことができる。

【０３３６】上記の認証において第１の局が正当とされた場合（図２０の処理１０１３）、第２の局４１の共有鍵生成手段９９は共有暗号鍵K_{12}を生成する（図２０の処理１０１４）。また、第２の局４１は、通信許可信号”ＯＫ”を中間局１６１に送信する（図２０通信１００５）。

【０３３７】通信許可信号”ＯＫ”を受信した中間局１６１は、通信許可信号”ＯＫ”を第１の局１１に送信する（図２０の通信１００６）。

【０３３８】通信許可信号”ＯＫ”を受信した第１の局１１は、共有暗号鍵生成手段２３を用い共有暗号鍵K_{12}を生成し（図２０の処理１０１５）、これを共有鍵格納部２７に格納する。

【０３３９】この第１０の実施の形態によれば、秘密情報を共有しかつ認証情報と共有鍵の生成手段とを持つ第１の局および第２の局の間に、秘密情報を持たない中間局が介在しても、第１の局の認証を実現することができ、然も第１の局および第２の局の間での暗号鍵の共有を実現することができる。

【０３４０】またこの第１０の実施の形態の場合も、認証の際に用いた情報を用いて第１の局および第２の局の間に暗号鍵の共有を実現している。しかも、第１の局の認証処理と、第１の局および第２の局の間の共有暗号鍵の生成処理とを連続的に行なうことができる。

【０３４１】また中間局に乱数発生の仕事を受け持たせたので、第１および第２の局の負荷を軽減することができる。

【０３４２】上述においてこの出願の各発明の実施の形態について説明した。しかしこれら発明は、上述の実施の形態に何ら限定されるものではなく、多くの変形または変更を行うことができる。

【０３４３】たとえば、一方向性関数f_i（ｘ，ｙ）の変数利用形態として、f_i（ｘ｜ｙ）、f_i（ｘＡＮＤｙ）、f_i（ｘＸＯＲｙ）などの形を使用しても良い。

【０３４４】が使える。ただし、ｘ｜ｙは連結を意味する。

【０３４５】また、第４～第７の各実施の形態では、共有暗号鍵を生成するとき、乱数ｒ（あるいはr_2）が暗号文で送られているため秘密情報を使わずにg_j（ｒ）（あるいはg_j（r_2））を共有暗号鍵としているが、共有暗号鍵を生成するとき秘密情報K_a（K'_a）を変数に加えれば安全性がさらに高められる。

【０３４６】また、第４の実施の形態では暗号アルゴリズムの暗号化鍵として秘密情報K_aを使い、また、第５～第７の各実施の形態では暗号アルゴリズムの暗号化鍵としてf_i（r_1，K_a）を使っている。しかし、暗号アルゴリズムによっては鍵の長さが合わないかも知れない。例えば、一方向性関数がＭＤ５の場合には、鍵であるf_i（r_1，K_a）が１２８ビットとなる。このとき暗号化アルゴリズムとしてＤＥＳ－ＣＢＣを用いたとすると、この鍵は長すぎる。そのような場合の対応方法として、鍵が必要以上に長い場合は上位ビットを切り捨てるか、短い場合は上位ビットに０を入れるなどの方法がある。E_q｛r_2，I_a｝、E_q｛r_2，I_a｜n_a｝の中の乱数についても、それが暗号化アルゴリズムE_q

に対し長かったり短かったりした場合は上記と同じ扱いとすることができる。

【０３４７】

【発明の効果】上述した説明から明らかなように、この出願の認証方法の各発明によれば、ユーザ情報と秘密情報とを用いて第１の局を第２の局（または第３の局）が認証することができる新規な方法が実現できる。このため、暗号通信に当たって正当な通信相手を確認することできる。

【０３４８】また特に、　：第１の局から送信されてきた乱数が乱数履歴に含まれるか否かを調べる処理を含む発明、　：第１の局によるアクセス回数が不等式関係を満たすか否かを調べる処理を含む発明、　：第１の局から送信された認証情報から復号した乱数が乱数履歴に含まれるか否かを調べる処理を含む発明、　：第１の局から送信された認証情報から復号したアクセス回数が不等式関係を満たすか否かを調べる処理を含む発明それぞれは、１度通信で用いた情報を再度通信に利用することを排除することができる。そのため、第３者が通信情報を盗聴してこれを利用して通信システムを攻撃しようとしても、それを防止することができる。

【０３４９】またこの出願の暗号鍵共有方法の各発明によれば、認証方法において用いた情報の１または複数をそのまま利用して共有暗号鍵を生成でき、しかも、認証方法の生成処理に連続して共有暗号鍵を生成することができる。認証処理が終えた後に共有暗号鍵生成のための通信を別途に行なう場合、この別途の通信の際に盗聴を受ける等の危険があるが、この発明の暗号鍵共有方法ではそれを防止することができる。

【０３５０】また、この出願の通信システムの各発明によれば、対応する認証方法の発明や対応する共有暗号鍵の生成方法の発明を容易に実施することができる。

【図面の簡単な説明】

【図１】第１の実施の形態の通信システムの構成説明図である。

【図２】第１の実施の形態の通信システムの動作説明図である。

【図３】第２の実施の形態の通信システムの構成説明図である。

【図４】第２の実施の形態の通信システムの動作説明図である。

【図５】第３の実施の形態の通信システムの構成説明図である。

【図６】第３の実施の形態の通信システムの動作説明図である。

【図７】第４の実施の形態の通信システムの構成説明図である。

【図８】第４の実施の形態の通信システムの動作説明図である。

【図９】第５の実施の形態の通信システムの構成説明図である。

【図１０】第５の実施の形態の通信システムの動作説明図である。

【図１１】第６の実施の形態の通信システムの構成説明図である。

【図１２】第６の実施の形態の通信システムの動作説明図である。

【図１３】第７の実施の形態の通信システムの構成説明図である。

【図１４】第７の実施の形態の通信システムの動作説明図である。

【図１５】第８の実施の形態の通信システムの構成説明図である。

【図１６】第８の実施の形態の通信システムの動作説明図である。

【図１７】第９の実施の形態の通信システムの構成説明図である。

【図１８】第９の実施の形態の通信システムの動作説明図である。

【図１９】第１０の実施の形態の通信システムの構成説明図である。

【図２０】第１０の実施の形態の通信システムの動作説明図である。

【符号の説明】

１１：第１の局
１３：秘密情報格納部
１５：ユーザ情報格納部
１９，４７：関数ｆテーブル（所定のアルゴリズムを複数記憶する手段）
２１：第１の認証情報生成手段
２３：共有鍵生成手段
２５、５５：関数ｇテーブル（暗号鍵生成アルゴリズムを複数記憶する手段）
２９：乱数生成手段
３１：アクセス回数計数手段
３３：認証情報生成手段（暗号化部）
３５、７１：アルゴリズムＥテーブル（暗号化アルゴリズムを複数記憶する手段）
４１：第２の局
４３：ユーザ情報・秘密情報格納部
４９：乱数生成手段
５１：第２の認証情報生成手段
５３：共有鍵生成手段
６１：乱数認証手段
６３：ユーザ情報・乱数履歴情報・秘密情報格納部
６５：アクセス回数認証手段
６７：ユーザ情報・アクセス回数・秘密情報格納部
６９：認証情報復号化手段
７３：認証手段
７５：復号鍵生成手段

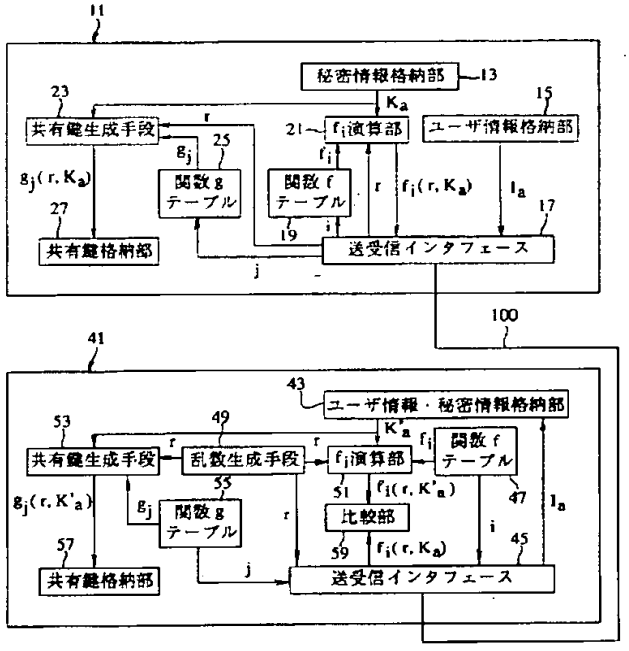
69

７７：認証情報復号化手段
７９：認証手段
８１：第１の乱数を認証する手段
８３：認証手段
１００、１００ａ～１００ｄ：通信回線
１２１：乱数生成手段
１２３：暗号文生成手段

70

１２５：暗号鍵生成手段
１２７：認証情報生成手段
１２９：暗号化手段
１３１：認証情報生成手段
１３３：暗号文生成手段
１５１：第３の局
１６１：中間局

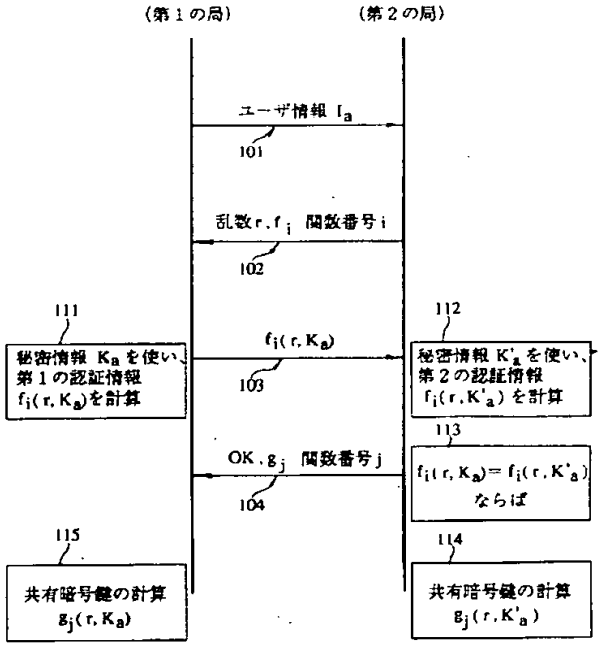
【図１】



11：第１の局
21：第１の認証情報生成手段（f_i演算部）
41：第２の局
51：第２の認証情報生成手段（f_i演算部）
59：認証手段（比較部）
100：通信回線
I_a：ユーザ情報
r：乱数
K_a, K'_a：秘密情報

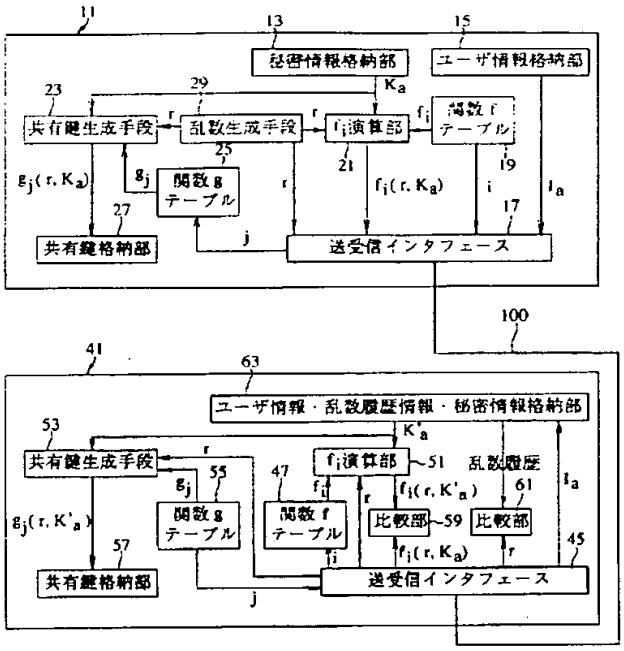
第１の実施の形態の通信システムの構成説明図

【図２】



第１の実施の形態の通信システムの動作説明図

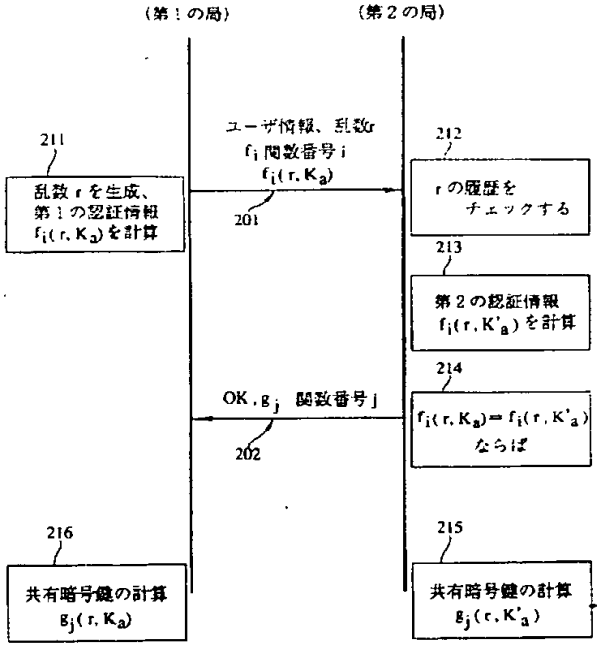
【図３】



61：乱数認証手段（比較部）

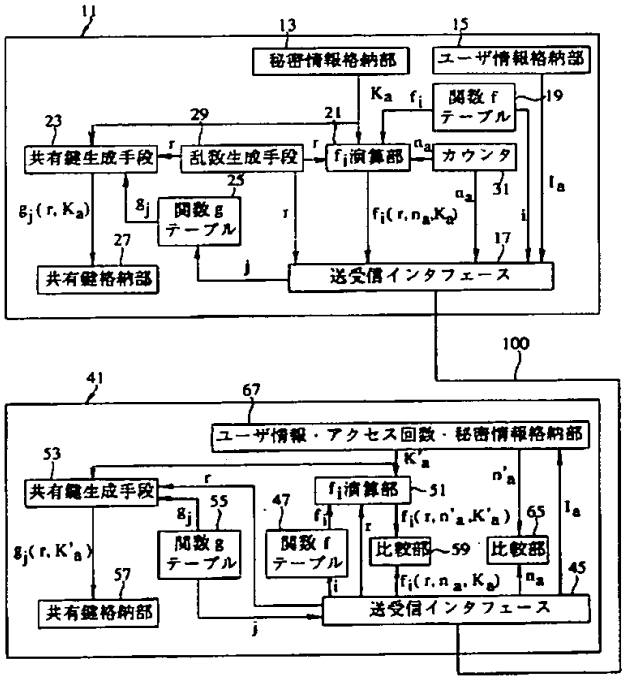
第２の実施の形態の通信システムの構成説明図

【図４】



第２の実施の形態の通信システムの動作説明図

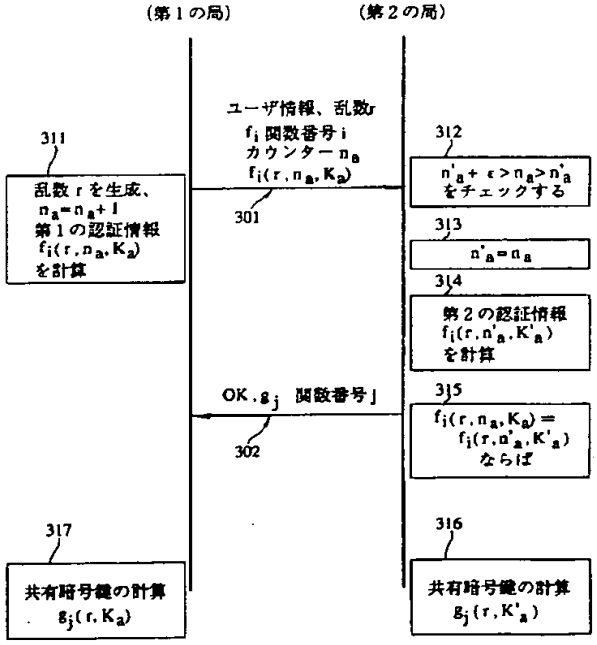
【図５】



31：アクセス回数計数手段（カウンタ）
65：アクセス回数認証手段（比較部）

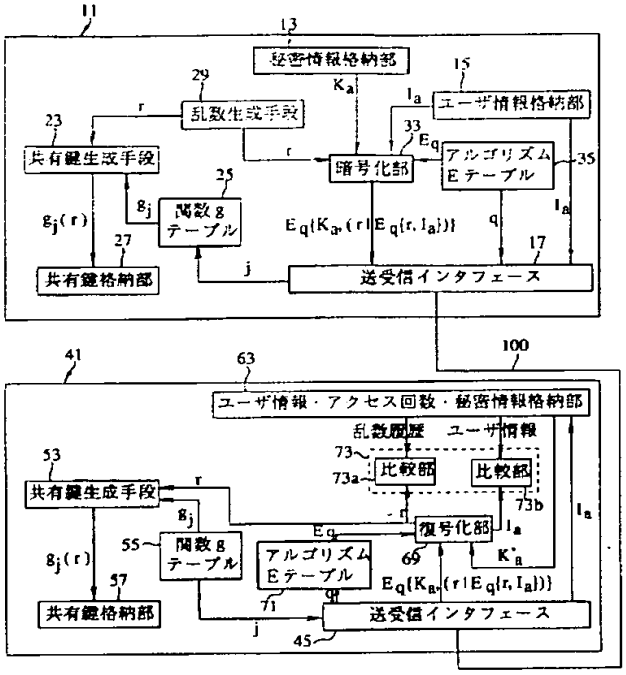
第３の実施の形態の通信システムの構成説明図

【図６】



第３の実施の形態の通信システムの動作説明図

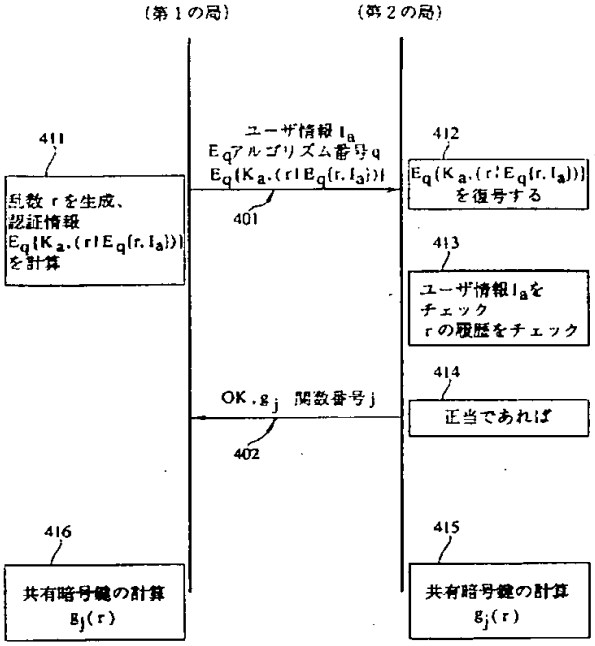
【図７】



33：認証情報生成手段　（暗号化部）
69：認証情報復号化手段（復号化部）
73：認証手段

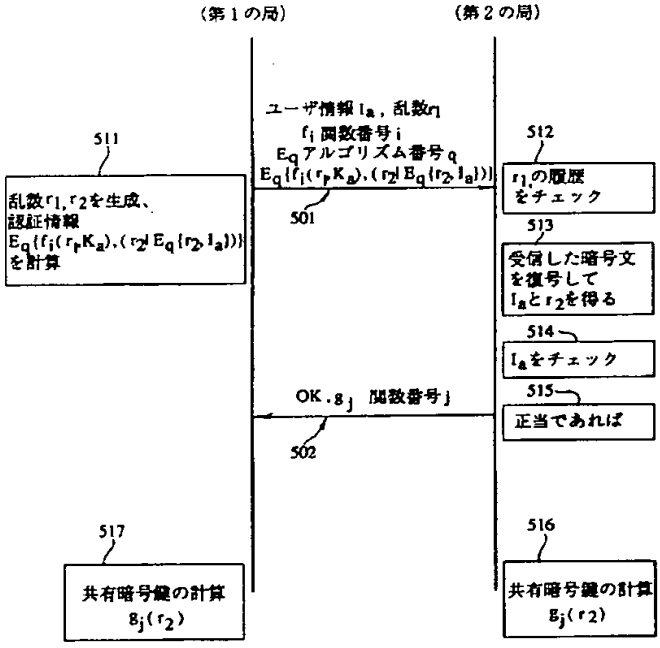
第４の実施の形態の通信システムの構成説明図

【図８】



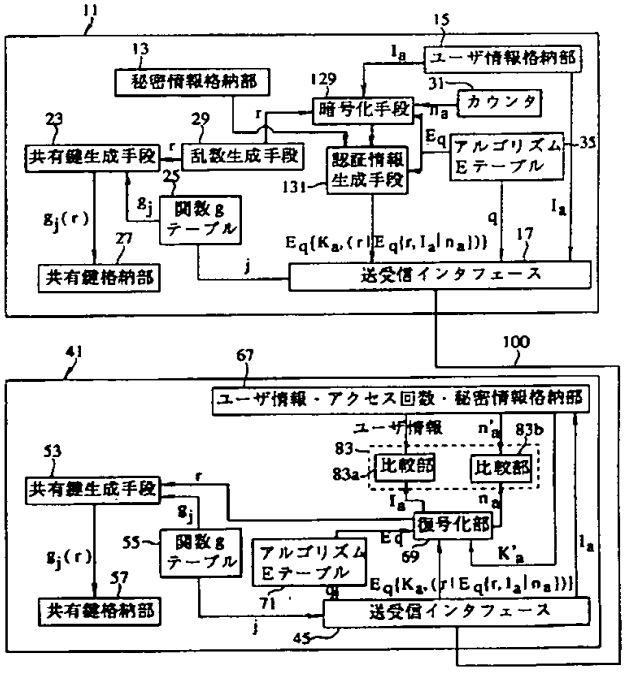
第４の実施の形態の通信システムの動作説明図

【図１０】



第５の実施の形態の通信システムの動作説明図

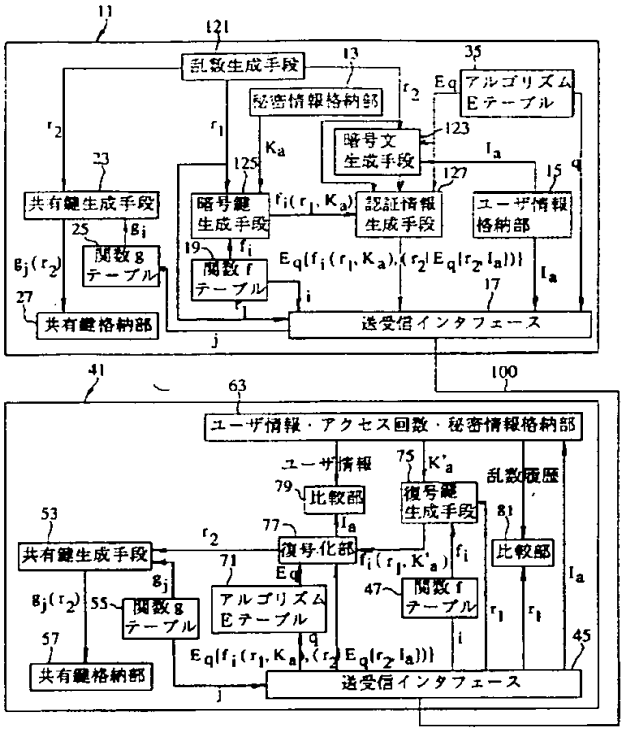
【図１１】



83：認証手段

第６の実施の形態の通信システムの構成説明図

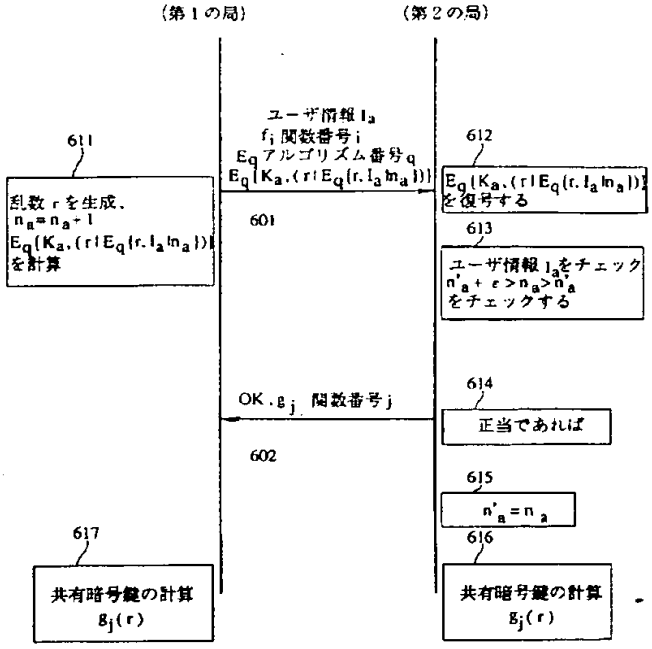
【図９】



77：認証情報復号化手段（復号化部）
79：認証手段（比較部）
81：第１の乱数を認証する手段（比較部）

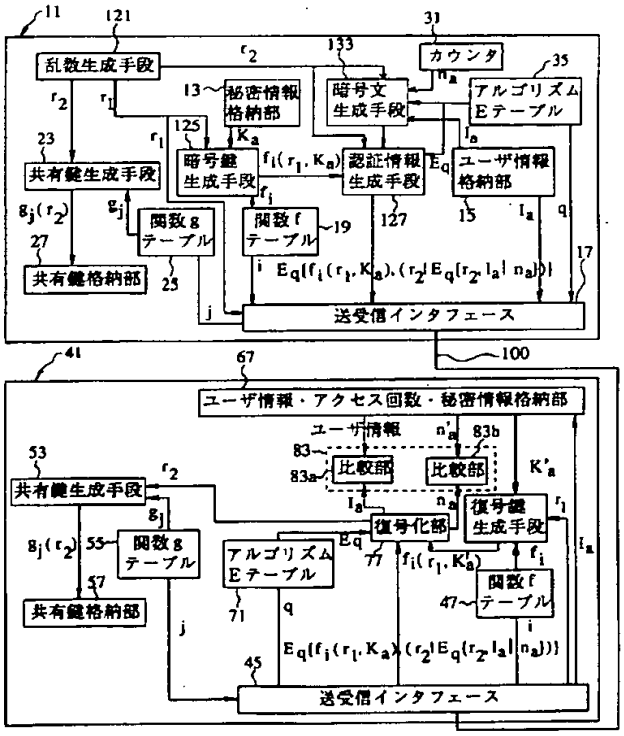
第５の実施の形態の通信システムの構成説明図

【図１２】



第６の実施の形態の通信システムの動作説明図

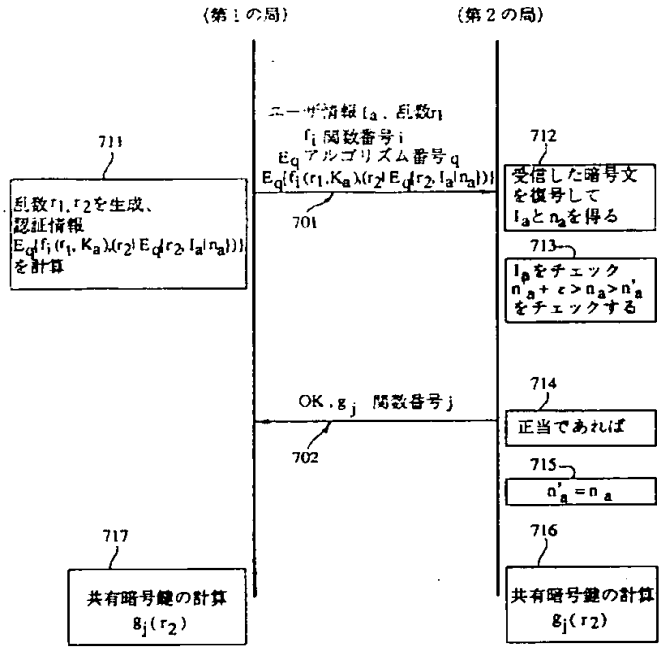
【図１３】



83：認証手段

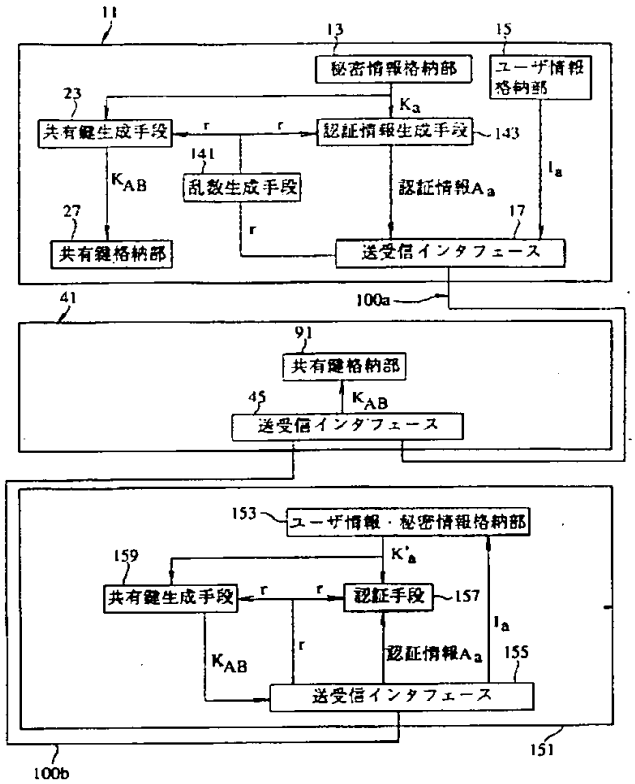
第７の実施の形態の通信システムの構成説明図

【図１４】



第７の実施の形態の通信システムの動作説明図

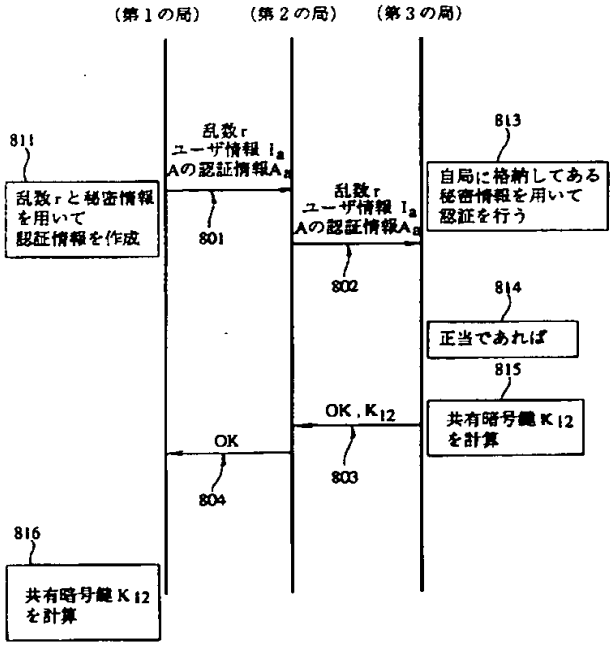
【図１５】



100a,100b：通信回線　　151：第３の局

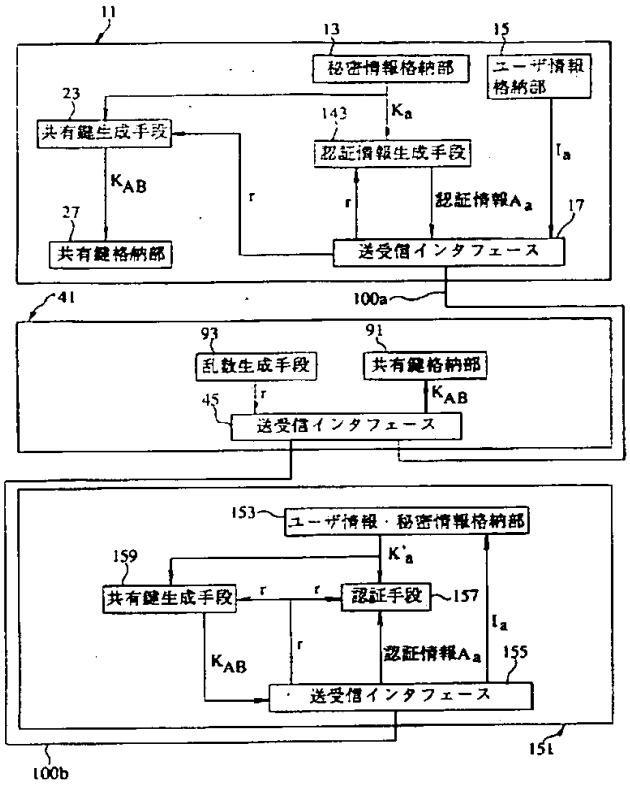
第８の実施の形態の通信システムの構成説明図

【図１６】



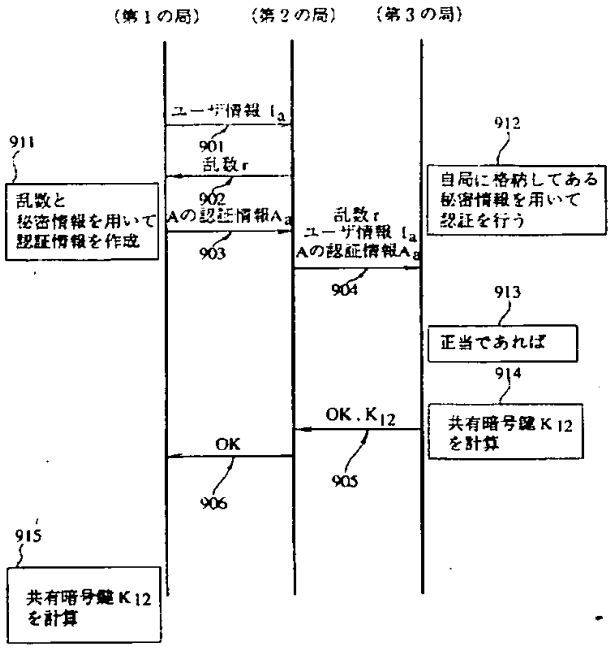
第８の実施の形態の通信システムの動作説明図

【図１７】



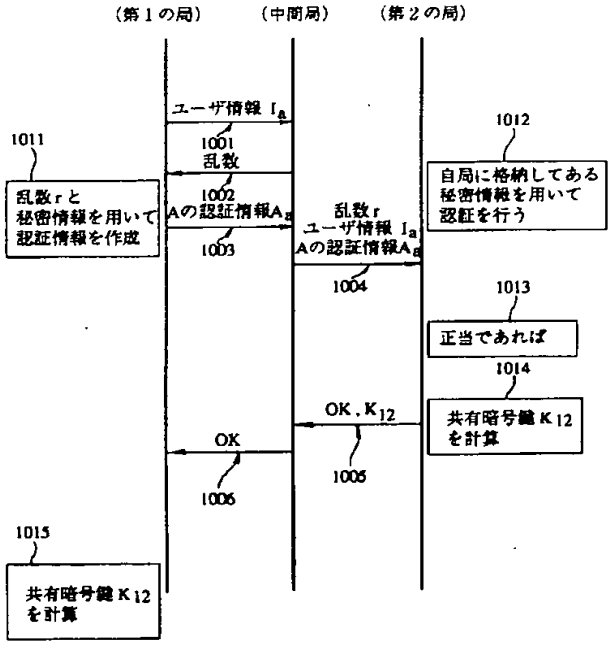
第９の実施の形態の通信システムの構成説明図

【図１８】



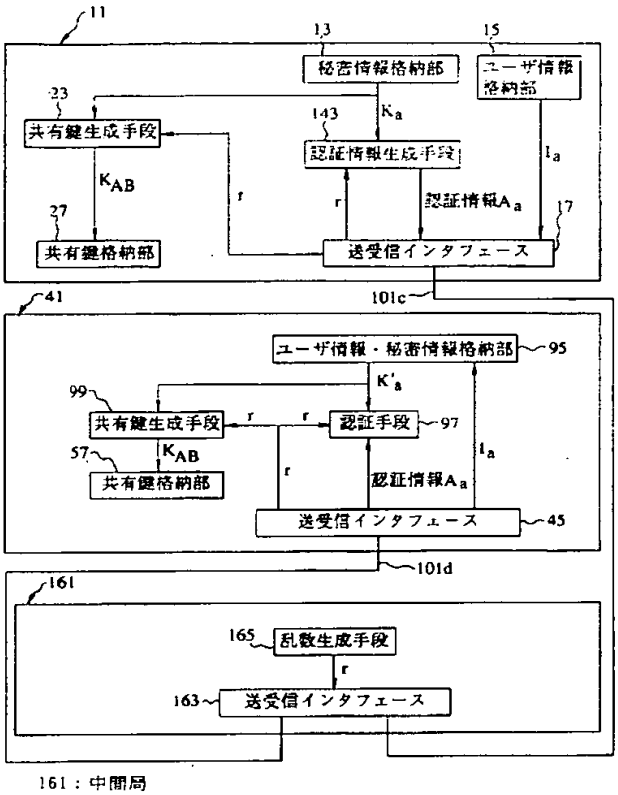
第９の実施の形態の通信システムの動作説明図

【図２０】



第１０の実施の形態の通信システムの動作説明図

【図１９】



161：中間局

第１０の実施の形態の通信システムの構成説明図

フロントページの続き

(72)発明者　鳥居　肖史
東京都港区虎ノ門１丁目７番12号　沖電気
工業株式会社内